Modernizing Your Group Policy Environment

Getting control of Windows Configuration Management

SDM Software, Inc.

March 2022

Overview

What is Group Policy Modernization? To understand that, it's important to know where Group Policy has come in the years since it was introduced in Windows® 2000. Group Policy's creation was a huge boon to Windows administrators. At last, centralized configuration control over Windows desktops and servers, tied to Active Directory and supporting fine-grained control over everything from security configuration to desktop lockdown. It was that fine-grained control—both in terms of the settings that you could configure in GP, as well as the dynamic and flexible targeting—that sowed the seeds for what would later be significant "sprawl" in most IT shops' Group Policy environments.

The concept of modernization is not new. We see it across many aspects of IT and even within the Windows world. You start out implementing a new technology and you learn many things over the course of its usage. In addition, the vendor (Microsoft) evolves the technology and its guidance around best practices as well. Fifteen years on, and you realize that **your** management of Windows configuration using Group Policy is…well…less desirable than it should be. Given that Group Policy has increasingly been used to secure your Windows desktops and servers, you need to have a good idea of what you've deployed and how it's working. **Group Policy Modernization** is about getting control of Group Policy and making sure it does what it's supposed to do.

Modernizing Group Policy—The Nuts and Bolts

Group Policy modernization is about systematically getting control of the cruft that has built up within your Windows configuration practices. It includes putting the tools and processes in place to prevent that cruft from building up again. If you are relying on Group Policy to harden your Windows servers and desktops, then modernization is imperative for protecting your organization's assets and ensuring that proper configurations are in place on your Windows systems. Based on years of experience, we've developed a methodology for getting to a modern, effective Group Policy deployment. The steps to Group Policy modernization are represented in Figure 1 below.

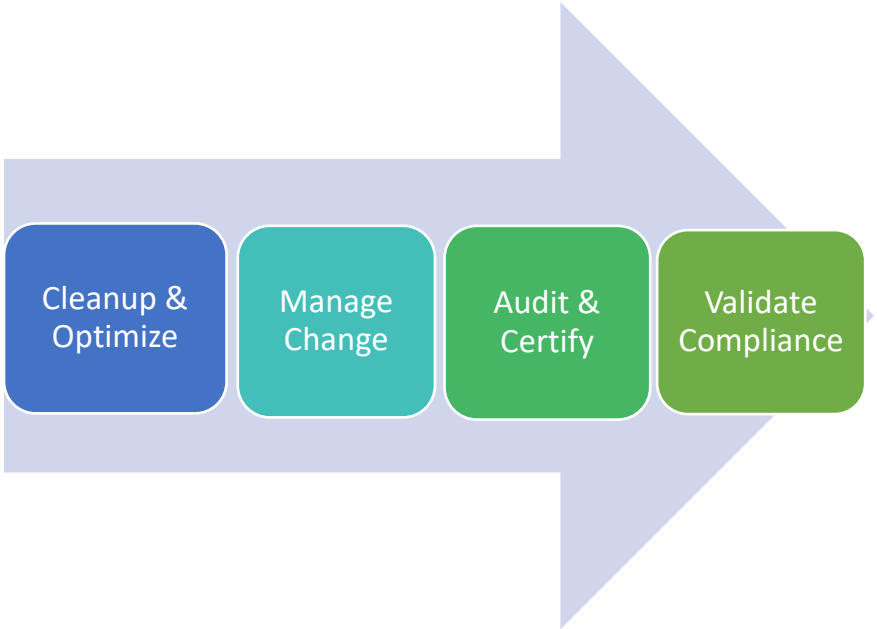


Figure 1 The Phases of Group Policy Modernization

The four phases above represent what we've experienced over the past many years of working with organizations and their Group Policy challenges. They represent the steps that a customer can take to get to Group Policy Modernization.

What should you expect when you are in a modernized Group Policy environment? What customers reap at the end of this process is five fold:

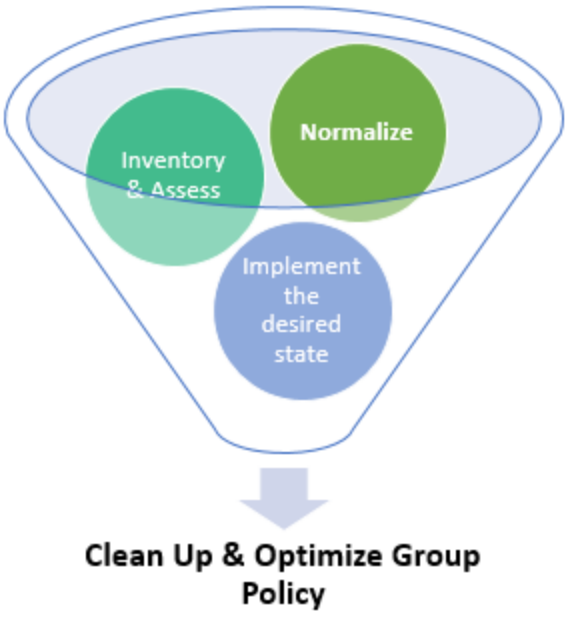
1. **Reliability:** Configuration management for Windows servers and desktops that they expect to be delivered is delivered, every time.
2. **Security:** Group Policy can be a vector for attack from bad actors. Many of these problems relate to changes to GPOs that go unchecked. A good change management process that tightly controls GPO and container delegation ensures that Group Policy won't be abused by attackers.
3. **Auditability:** A mechanism to inform them when changes happen to configuration items in the environment—change auditing and control practices that ensure they always know when a configuration is changing—this helps security and ensures that even with a good change control process, changes aren't circumventing that.
4. **Compliance:** Artifacts to provide auditors and compliance officers that show that numbers 1 and 2 above are indeed happening.
5. **Confirmation:** The ability to **see** what is happening from a configuration management perspective, across all Windows desktops and servers, and **know** that they are in compliance.

These five capabilities seem to be basic expectations of configuration management systems, but most Group Policy deployments we've seen fail to deliver on them. Let's dig in a bit to understand what the phases in Figure 1 really mean.

Phase 1: Clean Up and Optimize Group Policy

The first task of a modernizing effort is to get a handle on what you have today. GPOs often grow organically over the years in many organizations. Sometimes an administrator can't even tell us how many GPOs he/she has, let alone what they are all doing. If you're going to rely on GP to perform important tasks such as delivering security hardening onto Internet-facing web servers, it's wise to know what you have. When we work with customers in Phase 1, we start by helping them inventory and assess their existing environment—from basics like getting a count of GPOs, to understanding the settings in them.

The Clean Up and Optimize phase of modernization is composed of three sub-tasks, shown in Figure 2 below.



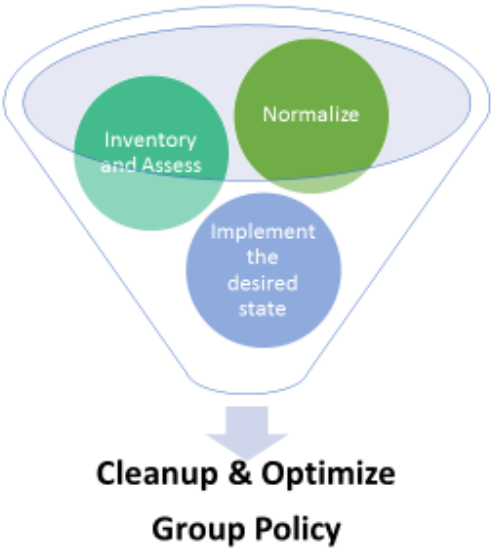


Figure 2 The three steps to Group Policy Cleanup and Optimization

SDM Software provides solutions for each of these three tasks, primarily through our **GP Reporting Pak** and GPO Migrator products. These products streamline and greatly speed the process of inventorying, analyzing and implementing the cleaned-up end state you are after—taking otherwise manual efforts from hours or even days, to minutes. Once you've assessed what you have using **GP Reporting Pak**, you can take that information and design an optimized structure for how you wish Group Policy to be in your environment. You're aiming for "normalized," which means reduced repetition and conflict within your

deployed GPOs. For the third sub-task, you can use the GPO Migrator to help drive those changes into your live environment—getting you to the desired state.

Phase 2: Manage Change

Once you have the optimized Group Policy configuration, the key is to keep it that way, and ensure that any changes related to Group Policy happen in a controlled and organized fashion. This is important both for operational and security reasons. Operationally, uncontrolled or accidental GPO changes or GPO linking modifications can cause outages and effect user productivity. From a security perspective, weaknesses in GPO or container delegation can allow an attacker to compromise GPOs, reduce your organization's overall security posture and leverage Group Policy to spread malware. What's required is a role-based change control process that ensures GPO and container changes are reviewed, approved and deployed by the correct staff.

Change Manager for Group Policy (CMGP) from SDM Software provides a modern, web-based platform managing change within your Group Policy infrastructure. CMGP provides for editors and approvers of GPOs and containers, allows for immediate or scheduled deployment of GPO and container changes, rollback of changes to both GPOs and containers and allows you to very precisely delegate and control change within your environment, to ensure both availability and security of your Windows environment.

Phase 3: Audit and Certify Your Group Policy Environment

Once Phase 2 is complete and you have a well-designed GPO change control process, you can safeguard against changes that try to happen outside of the change process. Good controls over GPO management are key. We have found three main actions that help to prevent GPO "sprawl" and the inevitable inconsistencies that arise from it: 1) Good change control process 2) up-to-date auditing of changes to the GPO environment, and 2) the assignment of ownership to any GPOs that are created/deployed. Change-auditing of all GPO management activities ensures that you always know when changes occur within your GP deployment, either within or outside of the change control process you've set up in Phase 2. This is critical if GP management is spread across multiple teams or IT administrators. The second item, assigning ownership to GPOs, requires that the GPO owners automatically certify, or attest, that their GPOs are still valid and useful in the environment. This provides a feedback mechanism that allows you to ensure that unused GPOs don't live within the environment forever, and that critical GPOs such as those used for security hardening are still configured as they need to be to do their job.

SDM Software created the **Group Policy Auditing & Attestation (GPAA)** product to address this phase of Group Policy modernization. GPAA provides real-time change auditing of all activities related to GPO management: creating, permissioning, linking and modifying GPOs. It also allows you to assign owners to GPOs of your choosing. Those owners are then emailed to periodically certify, or attest, that the GPOs are still valid in the environment. Administrators can then track their responses to help prevent GPO sprawl.

Phase 4: Validate Group Policy Compliance

After the first three phases, to clean up and get control over your Group Policy environment, then you are almost there, almost to the point where you are getting full value and benefit from your investment in Group Policy as your Windows configuration management platform. The final step is to have confidence that the policies you've deployed are being **delivered** successfully. It also comprises being able to show that successful delivery to anyone that asks (e.g. an auditor or manager looking to prove

that security hardening is indeed in place). Group Policy is great technology, but it has always lacked a feedback mechanism. I refer to it as "push and pray" configuration management because you often don't know, after deploying a policy, when and whether it has reached its targets. This is especially important if you rely on GP, as many IT shops do, for critical security hardening and lockdown. Do you want to bank the security of your business on, "Well, I **think** that setting is on all my servers"? Probably not. So for us, a key part of completing the modernization of Group Policy is ensuring that Group Policy is actually doing its job. We do that with our **Group Policy Compliance Manager** (GPCM) product, which allows central collection of Group Policy processing health and settings data from all of your Windows desktops and servers, and a variety of reporting against that data. GPCM provides the feedback mechanism that Group Policy has been lacking, and is the critical final step in the Group Policy modernization process.

Summary

There's no question that Group Policy is powerful technology for Windows configuration management. The fact that it's still heavily used in IT shops all over the world, some 20+ years after its release, is a testament to its power. That said, it is complex and must be managed accordingly. Manage it with the four steps outlined in this whitepaper, and you'll be on your way to a healthy, modernized GPO environment. For more information on how SDM Software can help modernize your Group Policy environment, contact us at sales@sdmsoftware.com.