

Automated Group Policy Validation

Defining a security policy doesn't guarantee it will be effective or enforced. **Remedio does.**

Broken Order

Group Policy Objects (GPOs) are designed to give operators a mechanism for enforcing security & operational preferences across user & computer accounts in Windows environments.

In practice, however, GPO designations may fail to reach and take effect on their intended endpoints for a number of reasons, including:

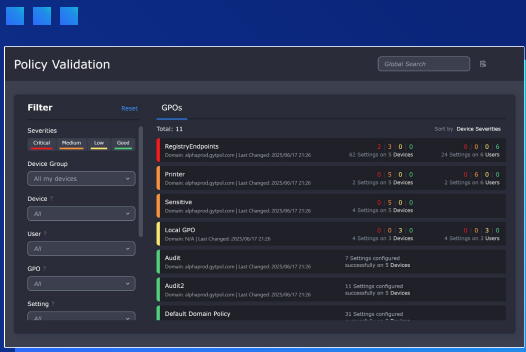
- Misconfigured loopback mode
- Group Policy Preferences (GPP) errors
- Item-level targeting (ILT) conflicts
- Missing ADMX templates
- OU filtering issues

These failures are common, hard to detect, and rarely validated in practice.



GPOs are Active Directory tools used to enforce system settings, security baselines, software deployments, user restrictions, and more.

Remedio validates GPO enforcement through continuous, deep inspection that compares current state device behavior to your intended policies.



The screenshot shows the 'Policy Validation' interface with a table of Group Policy Objects (GPOs). The table includes columns for GPO Name, Last Changed, Settings on Devices, and Settings on Users. The 'Registry/Endpoint' GPO is highlighted in red, indicating a failure.

GPOs	Settings on Devices	Settings on Users
Registry/Endpoint Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	62 Settings on 5 Devices	24 Settings on 6 Users
Printer Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	2 Settings on 5 Devices	2 Settings on 6 Users
Sensitive Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	4 Settings on 5 Devices	0 Settings on 6 Users
Equal GPO Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	4 Settings on 1 Device	4 Settings on 3 Users
Audit Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	2 Settings configured successfully on 5 Devices	0 Settings on 6 Users
Audit2 Domain: alpha01.gpol.com Last Changed: 2023/06/17 21:26	11 Settings configured successfully on 5 Devices	0 Settings on 6 Users
Default domain Policy	11 Settings configured	0 Settings on 6 Users

The Remedio Remedy

Unlike conventional tools, Remedio enforces secure configurations dynamically, ensuring policies are correctly implemented and maintained without disruption.

By streamlining hardening at scale, Remedio helps operators rapidly mitigate risks and prevent drift with minimal operational burden.

Consider the following examples...

	Risk	Root Cause & Fix
PowerShell and USB access not blocked for all users	Enables lateral movement and shadow admin activity	Misconfigured GPO loopback mode. Remedio identifies the issue and validates the corrected setting.
Passwords stored in Credential Manager	Credentials can be extracted by malware or attackers with local access	Item-Level Targeting filters conflict, preventing policy application. Filters are unified and validated by Remedio.
Firewall rules not enforced	Leaves open ports with no protection or alerting	ADMX template mismatch causes the GPO to fail silently. Templates are deployed and policies reapplied.
Local Policy overrides domain GPO	GPO settings appear to apply but are silently ignored	Local Group Policy on the endpoint takes precedence due to missing enforcement flag. Remedio flags the conflict; enforcement is corrected and confirmed.
Mapped printer or drive from GPP not applied to users	Users cannot access required network printer or the mapped driver	GPP item fails due to a network issue or denied access. Remedio detects the issue; targeting is corrected and validated across endpoints.

How It Works

Remedio leverages both Planning Resultant Set of Policy (RSOP) and Logging RSOP to identify field states that diverge from the intended application. The platform then determines the cause of that divergence and alerts the operator, empowering him/her to close the gap.

The process runs continuously to ensure the security of all monitored devices.

Here's how it works:

- Remedio's RSOP agent (installed only on a single Windows Server per domain) pulls Planning RSOP data from Active Directory using the GPMC API.
- Remedio's sensor (on each endpoint) collects Logging RSOP data, showing real GPOs applied to that machine.
- Both datasets are uploaded to Remedio's backend server (SaaS or on-prem).
- Comparing intent vs. reality across 30+ logical patterns, Remedio's rules engine detects:
 - Missing settings
 - Policy drift
 - ILT/precedence issues
 - ADMX/template mismatches
- Findings are packaged and presented in Remedio's severity-smart dashboard
- Guided remediation is provided for each alert.

Configuration Security Made Simple

With Remedio, it's easy to stay ahead of emerging threats – finding and fixing weaknesses in minutes rather than weeks.

Users enjoy the following benefits

- **Minimize Risk of Security Breaches:**
Detect GPO failures that could leave endpoints misconfigured and vulnerable to attack.
- **Ensure Compliance & Audit Readiness:**
Instantly prove that your security policies are not just defined — but effectively enforced across your environment.
- **Reduce Operational Costs:**
Save hours of troubleshooting with automated policy validation & root-cause analysis.
- **Improve IT Efficiency:**
Empower IT teams with fast, accurate visibility into policy drift and misapplication.
- **Support Strategic IT Initiatives:**
Confidently execute migrations, rollouts, and organizational changes with full GPO assurance.

About Remedio

Remedio is a first-of-its-kind solution focused on the configuration side of endpoint security.

Predicated on principles of automation and prevention, Remedio continuously monitors your devices and systems, detecting unpatched vulnerabilities and insecure configurations.

The platform enables proactive and non-disruptive remediation (or reversion) at the push of a button – ensuring safe and strict policy adherence while bolstering operational resilience and business continuity.

With Remedio, it's easy to bring any device or group in line with the standards of your choosing (e.g. CIS, NIST, etc.).

Additionally, Remedio helps organizations create and enforce golden image configurations – assuring consistent and secure baselines across all devices.

To learn more, please visit our website 

