

GROUP POLICY SECURITY.



A Group Policy Object is configuration that runs as SYSTEM on every computer it reaches and as the user at every sign-in; whoever can edit or link one holds that power. **Securing Group Policy means deciding who may write to its two stores, what may link where, and never leaving a secret in SYSVOL.**

- TWO STORES, ONE OBJECT
- TIER THE LINKS
- NO SECRETS IN SYSVOL
- AUDIT EVERY CHANGE

01 THE MECHANISM



Two Stores, One Object

A GPO is a container in the domain partition plus a template in SYSVOL on every domain controller, replicated by AD replication and DFSR, linked to sites, domains and OUs, applied by client-side extensions at startup and sign-in. **Both stores carry ACLs; both can be written.** [01]



Policy Is Execution

A modified GPO can plant scheduled tasks, services and accounts, disable tools or stage files on every computer it reaches. Computers refresh every 90 minutes plus a random offset, domain controllers every five. **An attacker with edit rights never touches the endpoint.** [02] [12]



The Rights That Matter

GPMC grants Read, Apply, Edit, or Edit/Delete/Modify security per GPO, plus link rights per site, domain and OU; Domain Admins own GPOs and Group Policy Creator Owners can make new ones. **Edit or link on anything reaching a domain controller is Domain Admin by another name.** [05] [15] [06]

02 THE FLOW

Harden the Estate

DESIGN

1

Start from a baseline: the Security Compliance Toolkit ships Microsoft's baselines for Windows 11, Windows Server, Microsoft 365 Apps and Edge as GPO backups, with Policy Analyzer to compare them against what you run; import through GPMC and link domain-controller policy only to the Domain Controllers OU. [07] [06]

2

Tier the links: GPOs linked to the domain root, the Domain Controllers OU and admin-host OUs are control-plane objects: edited only by Tier 0, from secure administrative hosts whose own GPOs require smart-card logon and restrict who may sign in. [06] [13]

3

Scope deliberately: shape OUs around administration, link most GPOs at the OU and password policy at the domain, narrow with security and WMI filtering. Since MS16-072 the computer reads user policy, so Domain Computers must keep Read or policy silently stops. [01] [11] [02]

Run It Safely

OPERATE

1

Purge secrets: MS14-025 removed the password fields from the Group Policy Preferences extensions (local users and groups, drives, services, tasks, data sources) but left existing values in place. Search SYSVOL for cpassword, rotate what you find, delete the items. [04] [03]

2

Audit the objects: enable Audit Directory Service Changes on domain controllers and set SACLs on policy objects and OUs, so a changed GPO raises event 5136 (class groupPolicyContainer) and a new link changes gPLink on the site, domain or OU; watch SYSVOL writes outside change windows. [09] [10] [16] [02]

3

Keep it rebuildable: keep a versioned Central Store (PolicyDefinitions-24H2, then swap names) so every console edits with the same templates, and run Backup-GPO -All on a schedule so Restore-GPO or Import-GPO can undo a bad change. [08] [14]

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Permissions	Per-GPO rights set with intent (Set-GPPermission), link rights held by few, Group Policy Creator Owners nearly empty, Domain Admins the owner.
Tiering	Domain-root, Domain Controllers and admin-host GPOs edited only by Tier 0 from secure hosts; domain controllers patched and managed separately.
Hygiene	No credentials in SYSVOL, baselines applied and compared, a current Central Store, scheduled GPO backups.
Visibility	Directory Service Changes auditing on domain controllers, alerts on 5136 for policy objects and gPLink, SYSVOL change monitoring, Policy Analyzer drift checks.

04 GPO RIGHTS COMPARED

RIGHT	SAFE TO GRANT WIDELY?	WHAT A HOLDER CAN DO
Read (GpoRead)	Yes	See every setting, including any secret left in SYSVOL; required for policy to apply since MS16-072.
Apply (GpoApply)	Yes	Be targeted by the GPO; security filtering is this right, so narrow it to groups rather than removing Read.
Edit settings (GpoEdit)	No	Change what every targeted computer runs as SYSTEM: tasks, services, accounts, user rights.
Edit, delete, modify security	No	All of the above, plus re-ACL the GPO to hand the same power to anyone.
Link or unlink on a site, domain or OU	No	Point any GPO, including a fresh one from Group Policy Creator Owners, at domain controllers or admin hosts.

GROUP POLICY SECURITY.

RESTRICT · TIER · AUDIT

05 PROGRAM OPERATIONS

Inventory who can write to policy.

Enumerate per-GPO permissions, link rights on the domain and every OU, and Group Policy Creator Owners membership; ATT&CK's mitigation is to find and correct GPO permission abuse paths with tools such as BloodHound. Remove Edit from anything that reaches a domain controller unless the holder is Tier 0. [02] [05] [15]

Treat the default GPOs and the Domain Controllers OU as crown jewels.

Change them only through change control, from administrative hosts; keep domain-controller RDP limited to jump servers by GPO, and patch and manage domain controllers separately from the general estate. [06] [01]

Hunt legacy preferences.

Search Groups.xml, Drives.xml, ScheduledTasks.xml, Services.xml and DataSources.xml under SYSVOL for cpassword; the AES key is public, so any domain user can decrypt them. Patched consoles cannot create new ones, but old items persist until you delete them. [03] [04]

Alert on policy change, not just on policy.

Microsoft's baseline enables Directory Service Changes on domain controllers; monitor 5136 by object class and attribute, correlate with 5137 creations, and treat SYSVOL writes from unexpected accounts or hosts as incidents. [09] [10] [02]

06 CONTROL MAPPING

ATT&CK

T1484.001 Group Policy Modification: M1047 audit and correct GPO permission abuse opportunities, M1018 WMI and security filtering; DET0305 detects GPO container and SYSVOL file changes. T1552.006 Group Policy Preferences: M1047 search SYSVOL and remove stored credentials, M1051 apply KB2962486. [02] [03]

MICROSOFT AD SECURITY

Securing domain controllers: GPOs linked to all domain-controller OUs restrict RDP to authorized users and jump servers, and patch management for domain controllers is separated from the general infrastructure. Secure administrative hosts: smart-card logon and logon rights enforced by GPOs linked to the admin-host OUs. [06] [13]

BASELINES AND TOOLING

The Security Compliance Toolkit holds Microsoft-recommended baselines in GPO backup format plus Policy Analyzer, LGPO and SetObjectSecurity; the Central Store in SYSVOL\Policies\PolicyDefinitions gives every administrator the same templates. [07] [08]

AUDITING

Microsoft's audit baseline sets Directory Service Access and Directory Service Changes to success and failure on domain controllers; event 5136 carries the object DN, class, attribute and old and new values, and Microsoft recommends monitoring it for sensitive objects. [09] [10]

07 WHAT THIS DOES NOT SOLVE

Devices Outside the Domain

Group Policy reaches domain members only; cloud-joined and unmanaged devices need MDM or local policy. **Know the gap.** [01]

The Editor's Workstation

Edit rights used from a compromised host are a compromised GPO. **Administer from secure hosts.** [13]

Replication Skew

Container and template replicate separately; a lagging domain controller serves stale policy. **Watch the version numbers.** [01]

Backups Fix Settings, Not Rights

Restore-GPO returns the settings; the permission that allowed the change is still there. **Fix the ACL too.** [14]

08 MYTHS VS. REALITY

MYTH	REALITY
"Only Domain Admins can change Group Policy."	Anyone with Edit on a GPO, link rights on an OU, or Group Policy Creator Owners membership can. [15] [05]
MYTH	REALITY
"The GPP password is encrypted, so it is safe."	The AES key is public and any domain user can decrypt it ; MS14-025 stopped new ones but left the old. [03] [04]
MYTH	REALITY
"Removing Authenticated Users tightens a GPO."	Since MS16-072 the computer reads user policy; without Read for Domain Computers it silently stops applying. [11]
MYTH	REALITY
"The Default Domain Policy is harmless."	It reaches every computer in the domain; Edit on it is domain-wide execution. [01] [02]
MYTH	REALITY
"Auditing is on by default."	Directory Service Changes is not; enable it on domain controllers and set SACLs or 5136 never fires. [09] [10]

09 SPEAK THE PROGRAM — KEY TERMS

GPC / GPT

The two halves of a GPO: the **container in Active Directory** and the **template in SYSVOL**.

SYSVOL

The replicated share on every domain controller holding policy files; **readable by every domain member**.

GPLINK

The attribute on a site, domain or OU listing the GPOs that apply; **changing it is linking**.

CPASSWORD

The Group Policy Preferences password field; **encrypted with a published key**.

SECURITY FILTERING

Granting Apply to specific groups so a GPO targets fewer principals; **Read must remain**.

CENTRAL STORE

SYSVOL\Policies\PolicyDefinitions: one set of ADMX/ADML templates **for every console**.