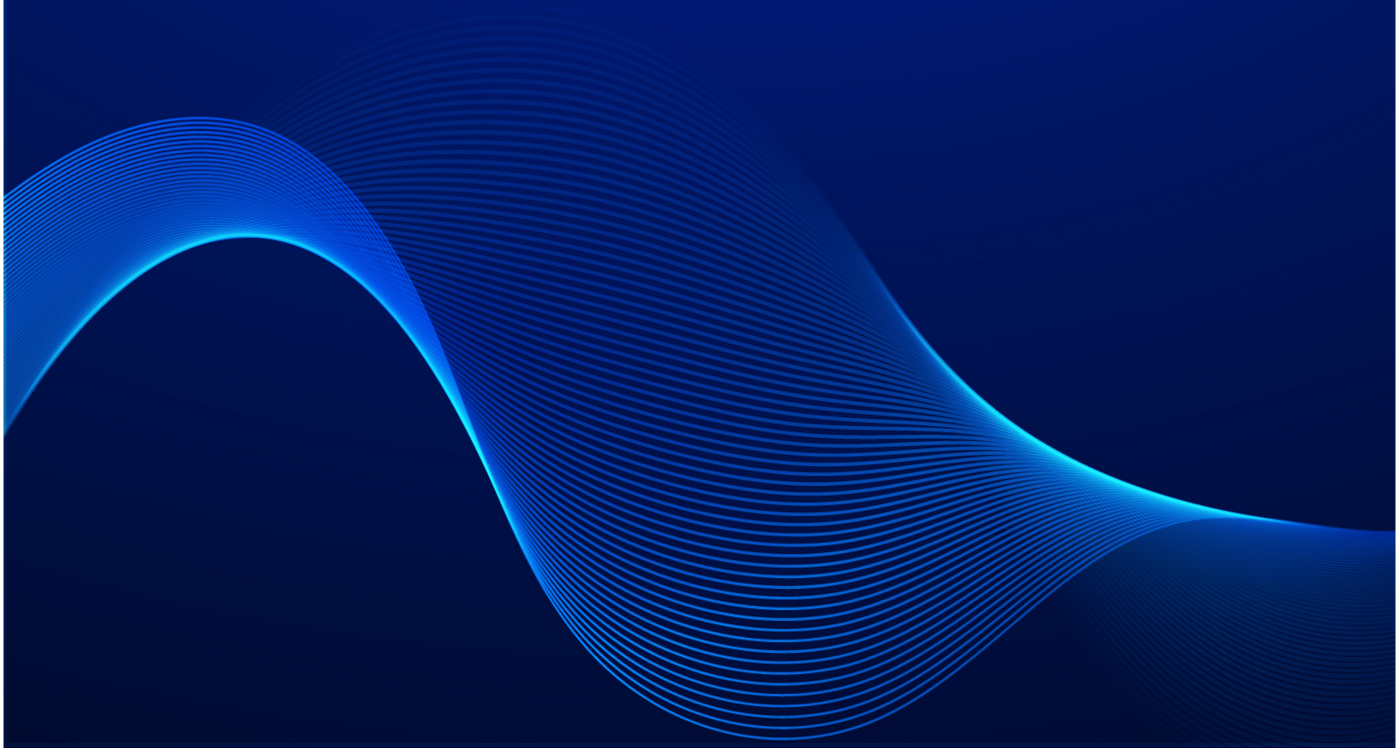
netwrix

Group Policy Best Practices



Group Policy enables organizations to control a wide variety of activity across the IT environment. For example, you can use Group Policy to prevent the use of USB drives, run a certain script when the system starts up or shuts down, deploy software, or force a particular home page to open for every Active Directory user in the network.

This guide provides both general Group Policy best practices and recommendations for specific settings. It also offers guidance for troubleshooting issues with your Group Policy objects (GPOs).

General Group Policy Best Practices

Establish separate organizational units (OUs) for users and computers

Having a good OU structure makes it easier to apply and troubleshoot Group Policy. In particular, putting Active Directory users and computers in separate OUs makes it easier to apply computer policies to all computers and user policies to all users.

Note that the root Users and Computers folders in Active Directory are not OUs. If a new user or computer object appears in these folders, move it to the appropriate OU immediately.

Use nested OUs for granular control

To delegate permissions to specific users or groups, put those objects in an appropriate nested OU (sub OU) and link the GPO to it. For instance, within the Users OU, you might create a sub OU for each department and link GPOs to those sub OUs.

Enforce a clear naming policy

Being able to determine what a GPO does simply by looking at the name will make Group Policy administration much easier. For example, you might use the following prefixes:

- **U** for GPOs related to users, such as U_SoftwareRestrictionPolicy
- **C** for GPOs related to computer accounts, such as C_DesktopSettings

Add comments to your GPOs

Add a comment to each GPO explaining its purpose and settings. This will make your Group Policy more transparent and easier to maintain.

Understand GPO precedence

Several GPOs can apply to the same Active Directory object at the same time. They are applied in a specific order, and new settings override those set by previously applied GPOs. This order LSDOU, which stands for:

- **Local:** Group Policy settings applied at the local computer level have the lowest precedence.
- **Site:** Settings for Active Directory sites are applied next.
- **Domain:** Next are Group Policy settings that affect all OUs in the domain.
- **OU:** Last applied are GPO settings at the OU level.

Create smaller GPOs for specific use cases

Align each GPO with a specific purpose, so it's easier to manage them and understand inheritance. Here are some examples of tightly focused GPOs:

- Browser Settings
- Security Settings
- Software Installation Settings
- AppLocker Settings
- Network Settings
- Drive Mappings

However, keep in mind that loading many small GPOs can require more time and processing at logon than having a few GPOs that each have more settings.

Set GPOs at the OU level rather than the domain level

Any GPO set at the domain level will be applied to all Active Directory objects in the domain, which could lead to some settings being applied to inappropriate users and computers. The only GPO that should be set at the domain level is the Default Domain Policy.

Instead, apply GPOs at the OU level. A sub OU inherits the policies applied to its parent OU; you don't need to link the policy to each sub OU. If you have users or computers that you don't want to inherit a setting, put them in their own OU.

Avoid blocking policy inheritance and policy enforcement

Blocking policy inheritance and policy enforcement make GPO management and troubleshooting much more difficult. Instead, strive for a well-designed OU structure that makes these settings unnecessary.

Instead of disabling a GPO, delete its link

Disabling a GPO will keep it from being applied to any OU in the domain, which could cause problems. Therefore, if a GPO is linked to a particular OU where you don't want it to be applied, delete the link instead of disabling the GPO. Deleting the link will not delete the GPO.

Avoid using the 'deny' permission in Group Policy

Administrators can explicitly deny a user or group the ability to be excluded from a specific GPO. While this functionality can be useful in certain scenarios, it can easily lead to unintended consequences because it will not be clear that a GPO is not being applied to certain objects. In order to find out which users or groups have been blocked; administrators would need to examine each GPO separately.

Implement change management and change auditing for Group Policy

Changes to GPOs can have profound effects on security, productivity, compliance and more. Therefore, all changes should be planned and fully documented. In addition, you should track all changes to Group Policy and get alerted to critical changes. Unfortunately, both these goals are difficult with native tools: The security logs do not provide a record of exactly which settings were changed, and getting alerts requires PowerShell scripting. For a more comprehensive and convenient approach, invest in a third-party solution like Netwrix Auditor for Active Directory.

To learn more about how to track changes to Group Policy, see the Group Policy Auditing Quick Reference Guide.

Speed GPO processing by disabling unused computer and user configurations

If you have a GPO that has computer settings but no user settings, you should disable the User configuration for that GPO to speed GPO processing time.

In addition, be aware of the following additional factors that can cause slow startup and logon times:

- Login scripts downloading large files
- Startup scripts downloading large files
- Mapping home drives that are far away
- Deploying huge printer drivers over Group Policy preferences
- Overuse of Group Policy filtering by Active Directory group membership
- User personal folders applied via GPO
- Use of Windows Management Instrumentation (WMI) filters (see the next section)

Avoid using a lot of WMI filters

WMI contains a huge number of classes with which you can describe almost any user and computer settings. However, using many WMI filters will slow down user logins and lead to a bad user experience. When possible, use security filters instead because they need less resources.

Use loopback processing for specific use cases

Loopback processing limits user settings to the computer that the GPO is applied to. A common use of loopback processing is when you need certain settings applied when users log into only particular terminal servers. You need to create a GPO, enable loopback processing, and apply the GPO to the OU that has the servers in it.

Use Advanced Group Policy Management (AGPM)

AGPM provides GPO editing with versioning and change tracking. It is part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance.

Back up your GPOs

Configure daily or weekly backup of policies using Power Shell scripting or a third-party solution so that you can always restore them to a known good state.

GPO Settings Best Practices

The following best practices will help you configure your GPOs to ensure strong security and productivity.

Do not modify the Default Domain Policy or the Default Domain Controller Policy

The Default Domain Policy affects all users and computers in the domain, so it should be used for account, account lockout, password and Kerberos policy settings only.

Use the Default Domain Controller Policy for the User Rights Assignment Policy and Audit Policy only.

However, it is even better to use separate GPOs even for the policies listed above.

Limit access to the Control Panel

It's important to limit access to the Control Panel on Windows machines. You can block all access to the Control Panel, or allow limited access to specific users using the following policies:

- Hide specified Control Panel items
- Prohibit access to Control Panel and PC settings
- Show only specified Control Panel items

Do not allow removable media

Removable media can be dangerous. If someone plugs an infected drive into your system, it unleash malware into the network. In addition, these drives are a path for data exfiltration.

You can disable the use of removable drives using the "Prevent installation of removable devices" policy. You can also disable the use of DVDs, CDs and even floppy drives if you want, though they present less risk.

Disabling automatic driver updates on your system

Driver updates can cause serious problems for Windows users: They can cause Windows errors, performance drop or even the dreaded blue screen of death (BSOD). Regular users can't switch updates off since it's an automated feature.

As an administrator, you can can disable automatic driver updates using the "Turn off Windows Update device driver searching" Group Policy. You will need the hardware IDs of the devices, which you can find in Device Manager.

Restrict access to the command prompt

The command prompt is very useful for system administrators, but enabling users to run commands could harm your network. Therefore, it's best to disable it for regular users. You can do that using the "Prevent access to the command prompt" policy.

Turn off forced restarts

If a user doesn't turn off their computer when they leave work and their machine is forcibly rebooted by Windows Update, they can lose their unsaved files. You can use Group Policy to disable these forced restarts.

Prevent users from installing software

Keeping users from installing software on their machines helps prevent a host of problems. You can prevent software installation by changing the AppLocker and Software Restriction settings and disabling extensions like ".exe" from running.

Disable NTLM authentication

The NTLM authentication protocol has a lot of vulnerabilities, including weak cryptography, so it is very vulnerable to attacks. Using Group Policy, you can disable NTLM authentication in your network and only the modern Kerberos protocol. However, first be sure to verify that no applications require NTLM authentication.

Block PowerShell locally

PowerShell is generally not needed by business users, and keeping them from using it can help prevent execution of malicious scripts. Using Group Policy, you can block the use of PowerShell on domain joined computers.

Admins who need to use PowerShell can be excluded from the policy. Alternatively, you can require them to run PowerShell scripts only on a designated machine for better security.

Disable guest accounts on domain computers

Guest accounts typically have limited access and functionality compared to regular user accounts, but they still pose important security risks. Disabling them using Group Policy helps prevent malicious users from gaining access to your environment.

Limit membership in the Local Administrators group

Members of the Local Administrators group can install software, delete system files, modify security settings and much more. This elevated access increases the risk of malware infections, accidental data loss and deliberate data exfiltration, and system instability and performance issues.

Using Group Policy, you can remove unnecessary accounts from the Local Administrators group on all computers.

Rename the local Administrator account

The Local Administrator account is a prime target for attackers because it provides privileged access on the machine. To reduce risk, it is a best practice to rename the Local Administrator account. In addition, use the account only when absolutely necessary; for routine tasks, use other administrative accounts with limited privileges.

Restrict anonymous access to named pipes and network shares

By default, named pipes and shares can be accessed anonymously, which can enable malicious actors to access sensitive data, such as confidential files, system information and network security settings. Accordingly, it is a best practice to use Group Policy to enforce restrictions on anonymous access to named pipes and shares across the network.

Enforce current password best practices

Standards bodies like NIST offer guidelines for password policy settings that reduce your risk from password-based attacks and credential reuse. You can use Group Policy to apply these recommendations in your environment.

Keep in mind that while stringent requirements for factors like password length, complexity and password age theoretically increase security, it doesn't always work that way in practice. Instead, such policies can lead users to adopt insecure workarounds like writing passwords down to avoid the hassle of account lockouts.

To get the full benefit of strong password policies, consider adopting a tool like Netwrix Password Secure, which will automatically create, store and enter credentials for users. That way, you can improve security by requiring passwords to be long, include special characters, be changed frequently and so on.

Disable anonymous SID enumeration

When anonymous SID enumeration is enabled, adversaries can gather information about user accounts and groups that is valuable in planning and executing cyberattacks. You can disable anonymous SID enumeration by modifying this registry setting:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

Be sure to back up the registry before making any changes, and exercise caution when editing registry settings. Changes should be performed only by knowledgeable and authorized personnel.

Prevent users from switching off Windows Defender

You should ensure that the built-in antivirus and antimalware protection remains active on all Windows systems. Go to the following path in the Group Policy Editor:

```
Computer Configuration > Administrative Templates > Windows Components > Windows
Defender Antivirus
```

Configure the Group Policy setting “Turn off Windows Defender Antivirus” as Disabled.

How Netwrix PolicyPak Can Help

Group Policy is an effective tool for detailed management of settings within a Windows environment. However, challenges such as the proliferation of Group Policy Object (GPO), organizational changes due to mergers, acquisitions, divestitures, fluctuating staff levels, and the formation of new entities have made its management increasingly difficult. Netwrix PolicyPak addresses these challenges by reducing GPO sprawl and streamlining the management process by merging multiple GPOs into fewer entities. This consolidation leads to improved login times, enhanced security, increased system reliability, and a reduction in configuration errors. Netwrix PolicyPak also enables administrators to deploy nearly 100% of Group Policy settings to Microsoft Intune without the added complexity of OMA-URI.

Group Policy Troubleshooting Tips

The following troubleshooting tips use help you investigate issues with Group Policy.

- In Windows 10 and Windows Server 2016, use the gpresult command to display Group Policy information for a remote user and computer, including how long it takes to process the GPO.
- Check the Event Viewer for any Group Policy-related errors or warnings.
- Use the Group Policy Results tool to see which policies are being applied to a specific user or computer, and which policies are not being applied.
- Use the Group Policy Modeling tool to simulate the application of Group Policies for a specific user or computer and identify any issues.
- Check that the affected user or computer is in the correct OU in Active Directory and that the Group Policy is linked to the correct OU.
- Check for any conflicting GPOs that may be overriding the desired settings using the Resultant Set of Policy (RSoP) tool.
- Use the Group Policy Management Console to check whether the user or computer has the necessary permissions to apply the GPO settings.

- Check for any network connectivity issues that may be preventing the user or computer from receiving the Group Policy settings.

- Review whether the Group Policy settings are configured correctly.

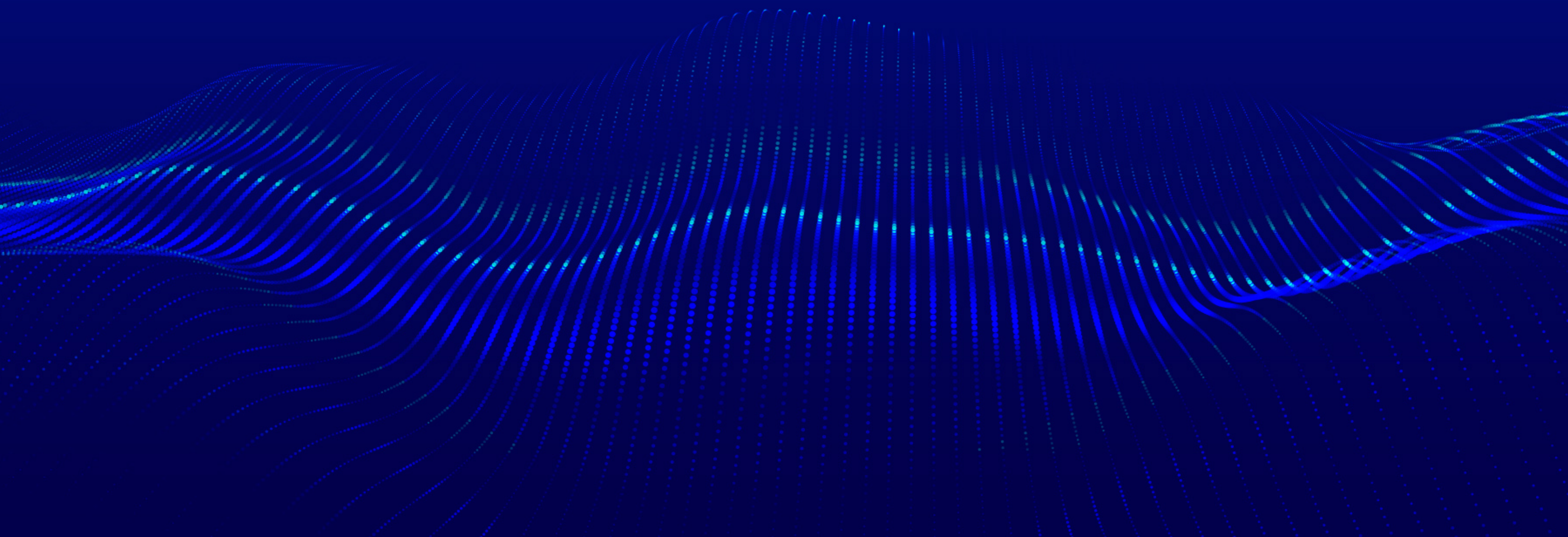
- For issues with Group Policy Preferences settings, use the Group Policy Preferences troubleshooting extension.

- If all else fails, consider resetting the Group Policy settings for the affected user or computer by running the "gpupdate /force" command or using the "Reset Group Policy Settings" option in the Group Policy Management Console.

Streamline Group Policy Management with Netwrix Solutions

- Gain visibility into your Group Policy settings.
- Get details about who changed what in your Group Policy and when each change was made.
- See before and after values for each Group Policy change.
- Eliminate GPO sprawl to make your Windows environment cleaner, easier to manage, and more secure.
- Pass compliance audits with less effort.

Request One-to-One Demo



About Netwrix Corporation

Netwrix makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,500 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity and infrastructure.

For more information, visit www.netwrix.com

Next Steps

See Netwrix products — Explore the full Netwrix portfolio: netwrix.com/products

Get a live demo — Take a personalized product tour with a Netwrix expert: netwrix.com/livedemo

Request a quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:	PHONES:
6160 Warren Parkway, Suite 100 Frisco, TX, US 75034	1-949-407-5125 Toll-free (USA): 888-638-9749
5 New Street Square, London EC4A 3TW	+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social