GPO

Lowell Vanderpool
TECH SAVVY PRODUCTIONS

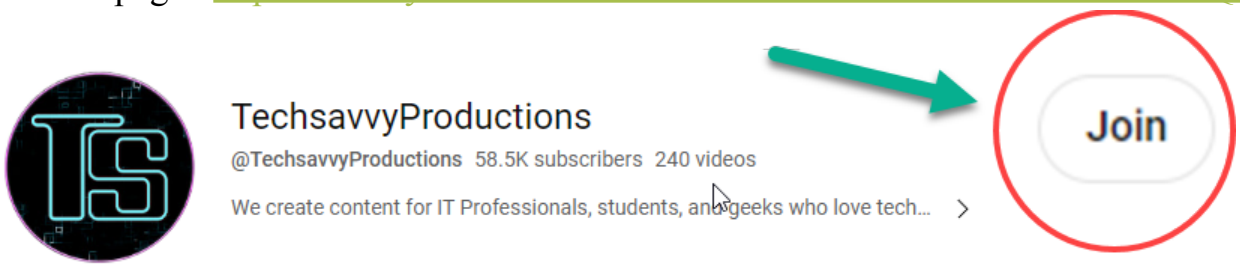
CONTACT US:

mrvanderpool@techsavvyproductions.com

SUPPORT US:

Please consider becoming a channel member:

- you get an early viewing of all our video content
- access to the complete series of videos for each subject
- links to video notes and PowerPoint slide deck both in MS-Word and PDF format
- Our eBook and resources folder
- Join our channel membership, it's $2.99/month); see the "Join" button on our channel homepage. https://www.youtube.com/channel/UCCAXBGYIJnScl0IFKXOIlsQ/join



"Everybody can be great... because anybody can serve. You don't have to have a college degree to serve. You don't have to make your subject and verb agree to serve. You only need a heart full of grace. A soul generated by love." Martin Luther King Jr.

.

SOCIAL MEDIA AND WEBSITE:

Check out our YouTube channel for more content!
YouTube: https://www.youtube.com/user/vanderl2796/featured
Check out our Website: https://www.techsavvyproductions.com
Facebook: https://www.facebook.com/TechSavvyTeamFL
Twitter: https://twitter.com/vanderl2796
Telegram: https://t.me/Lowell901
Mr.V Linkedin: https://www.linkedin.com/in/lowell-vanderpool-57970623/
Email: mrvanderpool@techsavvyproductions.com

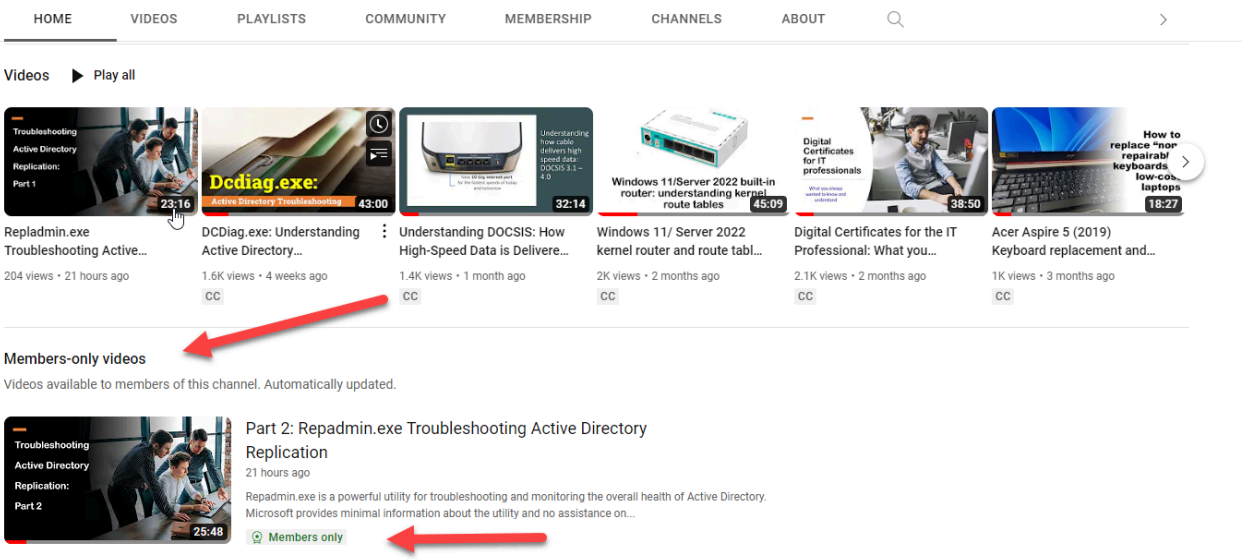
We translate subtitles on our videos into many languages:

Tech Savvy Productions

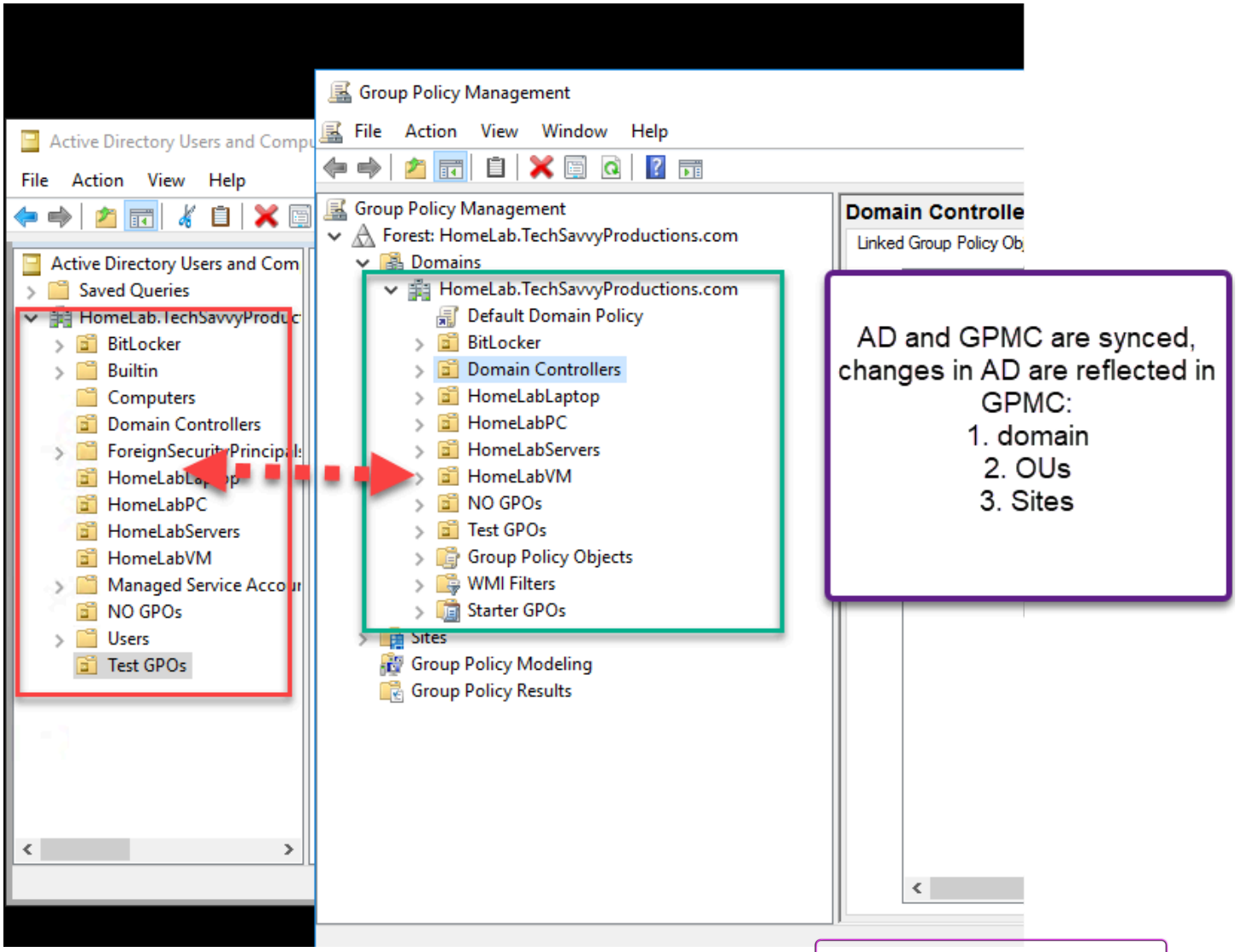
Two free ways to support our channel, like the video if it helped you better understand technology or the topic, and subscribe. Thank you for taking the time to do these helpful steps!

Where is member only resources?

Channel homepage and click on “Playlists” you will see a Members-only playlist.



Contents



Of *making many books there is no end, and much study wearies the body.*

Now all has been heard;
here is the conclusion of the matter:
Fear God and keep his commandments,
for this is the duty of all mankind.
For God will bring every deed into judgment,
including every hidden thing,
whether it is good or evil.

The Basics of Group Policies

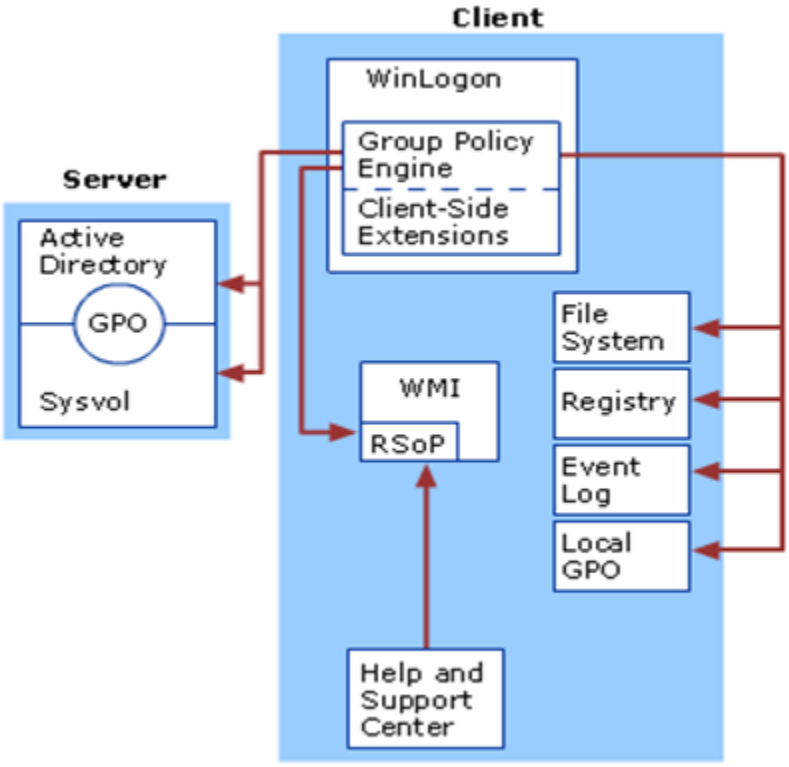
By

Craig Marcho
Published Mar 15 2019 05:16 PM 18.9K Views

The Performance team handles Group Policies for several different components - most notably Printing, Internet Explorer and Terminal Server. In most environments, the Active Directory administrator handles the design, implementation and maintenance all of the group policies - even if another group is responsible for the technologies affected by the policies. When an issue arises with one of these technologies, often it is the administrator for that system who is trying to troubleshoot the problem - who may not know much about the policies in place. So today we're going to go over some basic Group Policy concepts.

The primary purpose of Group Policy is to apply policy settings to computers and users in an Active Directory domain to enable IT administrators to automate one-to-many management of users and computers. This simplifies administrative tasks and reduces IT costs. Administrators can efficiently implement security settings, enforce IT policies, and distribute software consistently across a given site, domain, or range of organizational units.

The Group Policy engine is the infrastructure that processes Group Policy components including server-side snap-in extensions and client-side extensions. It is a framework that handles client-side extension (CSE) processing and interacts with other elements of Group Policy. The Group Policy engine is contained within userenv.dll which runs inside winlogon.exe. So let's take a quick look at the Group Policy architecture:



When a client logs in to the Active Directory, it processes the appropriate group policies based on its membership within the domain, within a specific group, or within an organizational unit. For example, if your machine is a member of an AD domain, then there will be a set of domain-wide policies that are applied to the machine when it is booted up. There may also be policies applied based on where the machine is located geographically, or based on which business unit the machine belongs to. The same principle applies to users.

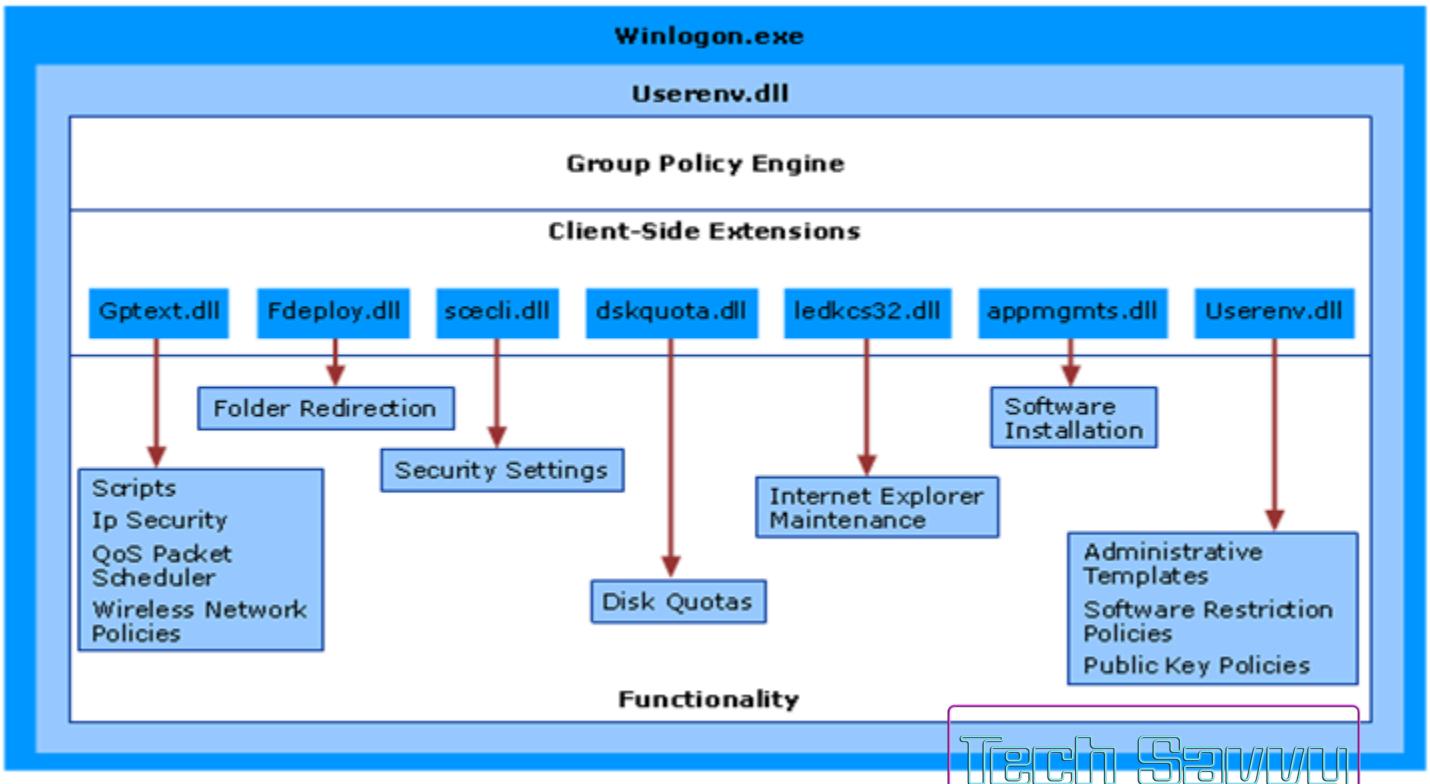
The Group Policy Objects themselves are located on the SYSVOL share of the domain controllers within the AD. Once the policies are brought down to the client, the individual client-side extensions (CSE) will apply the policies to the appropriate areas.

Client-Side Extensions (or CSE's) are called by the Winlogon process at computer startup, user logon and at the Group Policy refresh interval. Each CSE is registered with Winlogon in the registry. This registration information includes a DLL and a DLL entry point (function call) by which the CSE processing can be initiated. The Winlogon process uses these to trigger Group Policy processing. Each extension can opt not to perform processing at any of these points (for example, avoid processing during background refresh).

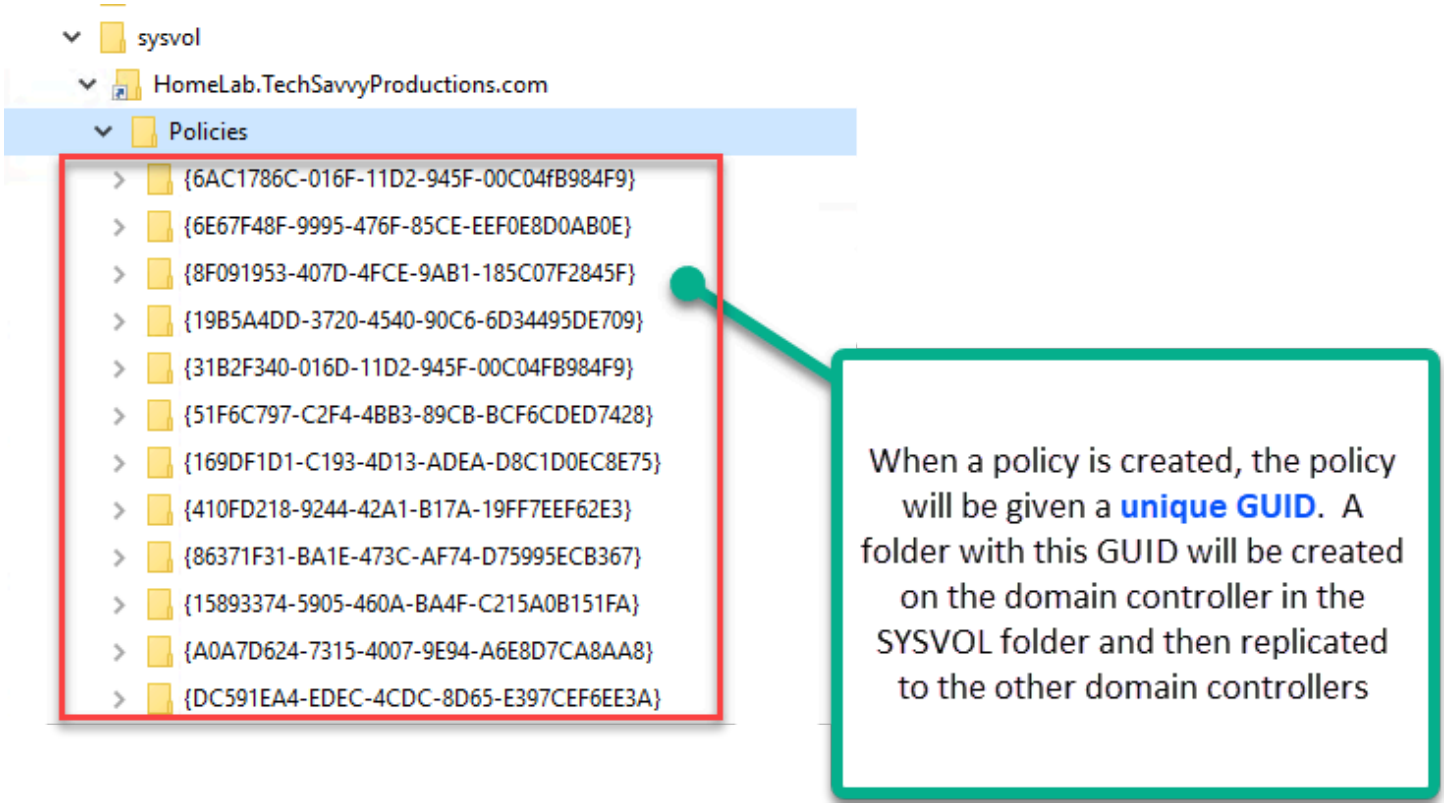
Each CSE is registered with Winlogon in the following registry key: *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\GPExtensions* . Each extension is identified by a key named after the GUID of the extension. Some common extensions and GUID's are shown below:

GUID	Extension Name
35378EAC-683F-11D2-A89A-00C04FBBCFA2	Administrative Templates
3610EDA5-77EF-11D2-8DC5-00C04FA31A66	Disk Quotas
B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A	EFS Recovery
25537BA6-77A8-11D2-9B6C-0000F8080861	Folder Redirection
A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B	Internet Explorer Maintenance
E437BC1C-AA7D-11D2-A382-00C04F991E27	IP Security
426031c0-0b47-4852-b0ca-ac3d37bfcb39	QOS Packet Scheduler
42B5FAAE-6536-11D2-AE5A-0000F87571E3	Scripts
827D319E-6EAC-11D2-A4EA-00C04F79F83A	Security
C6DC5466-785A-11D2-84D0-00C04FB169F7	Software Installation

The diagram below shows the Group Policy Client-side extension components.



When a policy is created, the policy will be given a unique GUID. A folder with this GUID will be created on the domain controller in the SYSVOL folder and then replicated to the other domain controllers.



The Group Policy template folder contains the following subfolders:

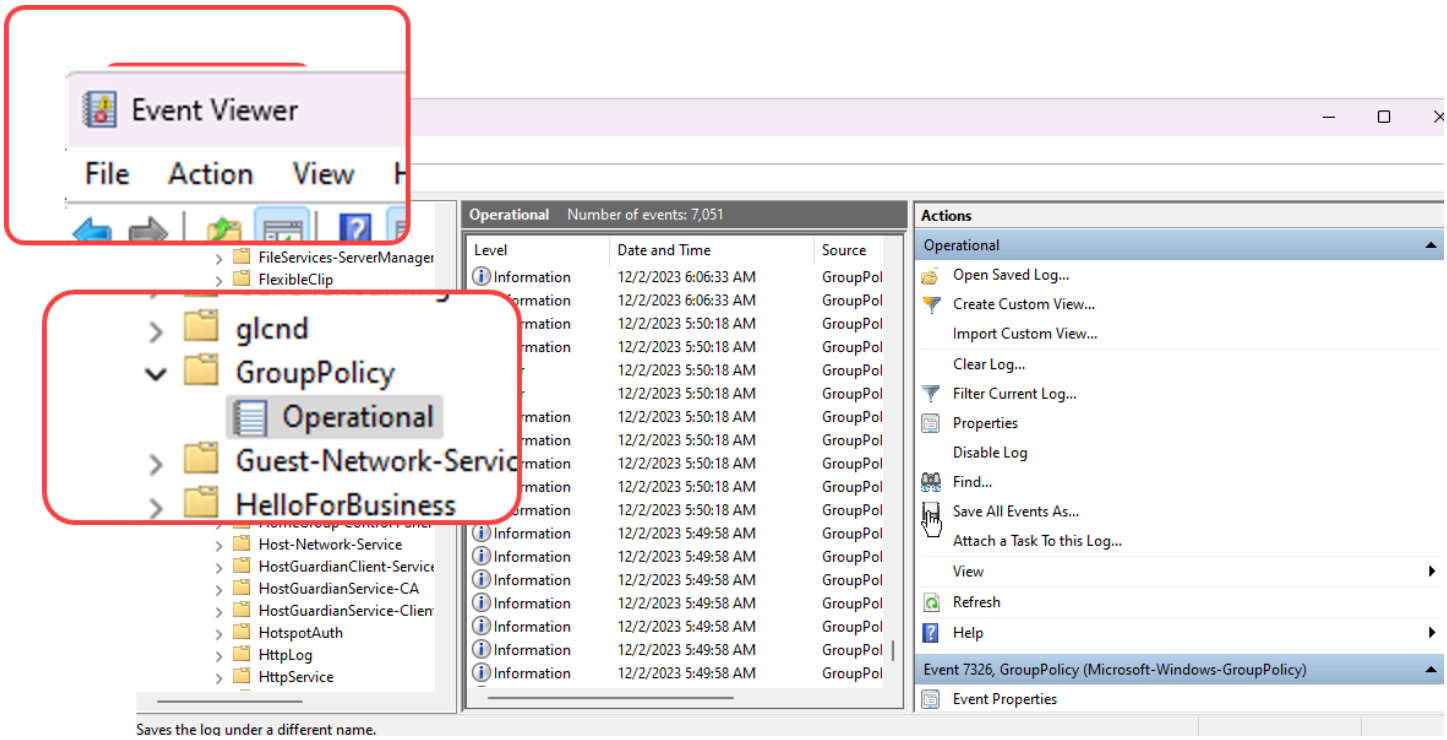
- ADMX: Contains all of the .admx files for the GPO
- Machine: Includes a Registry.pol file that contains the registry settings to be applied to computers (HKEY_LOCAL_MACHINE)
- User: Includes a Registry.pol file that contains the registry settings to be applied to users (HKEY_CURRENT_USERS)

The User and Machine folders are created at install time, and the other folders are created as needed when the policy is set. Each time GPOs are processed, a record of all of the GPOs applied to the user or computer is written to the registry.

- GPOs applied to the local computer are stored in the following registry path: *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History*
- GPOs applied to the currently logged on user are stored in the following registry path: *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\History*

OK - so now that you know a little bit about the behind the scenes workings of Group Policies, let's quickly cover some basic GPO tools. The three main tools to become familiar with are

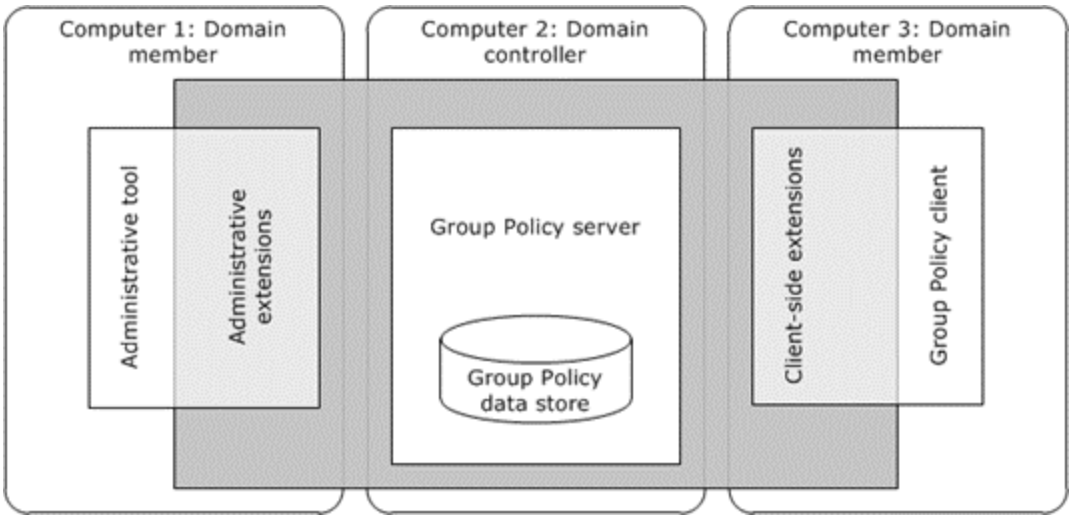
gpresult , the **userenv.log** and **Resultant Set of Policies Snap-in (rsop.msc)** . **GPResult** is a command-line utility that can be run with several different switches to determine what policies are applying (or might apply) to a particular user on the machine on which it is executed. The **Userenv.log** file is a diagnostic log to record detailed information about processing of the Group Policy engine. The logging is enabled via the registry in the following key: *HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon* . The specific value to set is *UserenvDebugLevel* . This value is a DWORD value that should be set to 0x10002 to enable verbose logging to a log file. The log file is written to the %Systemroot%\Debug\UserMode\Userenv.log file.



And that brings us to the **Resultant Set of Policies Snap-in (rsop.msc)** . All Group Policy processing information is collected and stored in a Common Information Model Object Management (CIMOM) database on the local computer. This information, such as the list, content, and logging of processing details for each GPO, can then be accessed by tools using Windows Management Instrumentation (WMI). The Resultant Set of Policies Snap-in leverages WMI to list the GPO details. RSOP functionality is only available on Windows XP / Windows Server 2003 and later Operating Systems

And that wraps up our overview of Group Policies. In future posts, we will be looking at GPO's as they pertain to Internet Explorer, Terminal Services and other technologies supported by the Performance team. Until next time ...

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gpod/6c634939-2ccf-4412-b75f-0035dc05ea67



Whoever of you loves life
and desires to see many good days,
keep your tongue from evil
and your lips from telling lies.
Turn from evil and do good;
seek peace and pursue it.

From a 10,000-foot view, Active Directory (AD) Group Policy Objects (GPOs)

are a powerful and integral part of the Microsoft Windows server ecosystem, providing centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. Here's an overview:

1. **Centralized Management**: GPOs allow administrators to manage the settings of users and computers across an entire organization from a central location. This eliminates the need for manual configuration of each individual machine or user account.
2. **Active Directory Integration**: GPOs are an integral part of Active Directory. They leverage the AD infrastructure for identifying which settings apply to which users and computers based on their AD objects, such as OUs (Organizational Units), domains, and sites.
3. **Policy Application**: GPOs are applied automatically when a user logs on or a computer starts up, and periodically in the background. They enforce specific configurations, security settings, and operational rules across the networked environment.
4. **Scalability and Flexibility**: The system is highly scalable, capable of managing configurations for a handful of computers or thousands in a large enterprise. It also offers flexibility in terms of targeting specific groups, users, or computers with tailored settings.
5. **Security and Compliance**: GPOs are essential for enforcing security policies and compliance standards across an organization. They control security settings, such as password policies, user rights, and access to resources.
6. **Group Policy Objects and Settings**: Each GPO can contain numerous individual settings related to user interface, network behavior, security, and more. These settings are divided into 'User Configuration' and 'Computer Configuration'.
7. **Hierarchical Application and Inheritance**: GPOs are applied in a hierarchical manner, with the possibility of inheritance and overriding at different levels like site, domain, and OU. This hierarchy allows for a granular application of policies.
8. **Customization and Flexibility**: Administrators can create custom GPOs tailored to specific needs. They can also use filtering and targeting to apply policies selectively.

9. **Lifecycle Management**: The life cycle of a GPO includes its creation, testing, deployment, monitoring, and eventual retirement or updating as organizational needs and technologies evolve.
10. **Tools and Reporting**: Various tools, including the Group Policy Management Console (GPMC), are available for creating, managing, and troubleshooting GPOs. Reporting and diagnostic tools help in analyzing policy settings and resolving issues.

In essence, AD GPOs provide a framework for efficiently and effectively managing the configuration and operation of a Windows-based network, ensuring that systems and users conform to the desired standards and policies set by the organization's IT department.

2.1.1 System Purpose

System administrators are required to provide consistency among groups of computers and/or users, with respect to such things as operating system versions, applications, and the general user experience. Group Policy enables a remote administrator to ensure that groups of computers conform to standards, and that users are provided with a consistent experience regardless of the computer that they use.

As the enabling technology in Windows, Group Policy allows programs and administrators to use Active Directory as an infrastructure to centralize network administration, centrally define management policy, and delegate administrative authority. Users, computers, devices, and resources are represented as objects in Active Directory. With Group Policy, administrators can target policy settings on everything from users and computers to individual objects throughout the Active Directory hierarchy.

Group Policy depends on a domain-joined environment, as described in section 2.4. In this environment, the Group Policy protocols enable a Group Policy client to retrieve GPO metadata and policy settings from a Group Policy server, and it enables the Administrative tool to create, retrieve, update, and delete policy settings. The Group Policy: Core Protocol [MS-GPOL] provides the core functionality of Group Policy, as described in section 1.1.1. Group Policy functionality is extensible on both the client side (policy application) and the administrative side (policy administration).

2.1.1.1 Core Protocol

The Group Policy: Core Protocol [MS-GPOL] is the main Group Policy protocol. It is a client/server protocol that allows clients to discover and retrieve policy settings created by Group Policy administrators. Policy settings are the directives that Group Policy administrators employ to control client behavior. Section 1.1.1 describes the Group Policy: Core Protocol in more detail.

2.1.2.1 Component Protocol Communications

The following diagram shows the Group Policy protocols along with the protocols that facilitate communication between components.

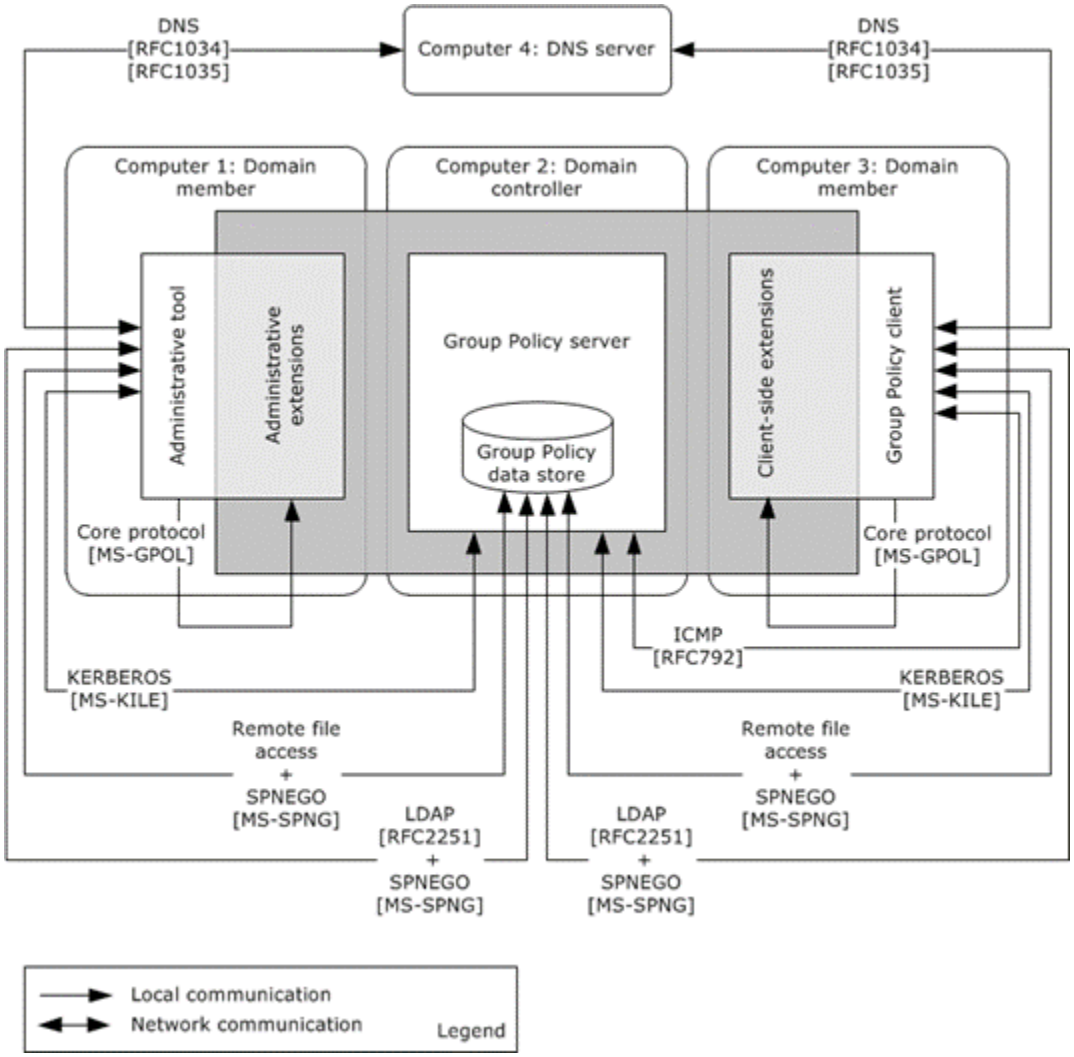


Figure 4: Group Policy component protocol communications

Group Policy makes use of several protocols to facilitate communications among its components, as illustrated in the preceding diagram:

Administrative Tool Communication Protocols

The Administrative tool uses the following communication protocols:

- LDAP ([RFC2251]) and a file access protocol for accessing Group Policy data store components, which includes the Active Directory data store on the Group Policy server and the Group Policy file share data store.

- DNS, as described in [MS-ADOD] section 3.1.1, for locating a domain controller.
- Kerberos [MS-KILE] or NT LAN Manager (NTLM) Authentication Protocol [MS-NLMP], as described in [MS-SPNG], for authenticating to the Group Policy server.
- Group Policy: Core Protocol [MS-GPOL], for invoking and processing Administrative tool extensions via the Administrative tool.

Group Policy Client Communication Protocols

The Group Policy client uses the following communication protocols:

- LDAP and a file access protocol, for accessing Group Policy data store components, which include the Active Directory data store on the Group Policy server and the Group Policy file share data store.
- DNS, as described in [MS-ADOD] section 3.1.1, for locating a domain controller.
- Kerberos [MS-KILE] or NTLM [MS-NLMP], as described in [MS-SPNG], for authenticating to the Group Policy server.
- Group Policy: Core Protocol, as described in [MS-GPOL], for invoking and processing CSEs via the core Group Policy engine.

Group Policy Extension Communication Protocols

The communication protocols that the Group Policy extensions use, which include Administrative tool extensions and CSEs, are as follows:

- LDAP and a file access protocol, for communicating with Active Directory and the Group Policy file share.

  In policy administration mode, Administrative tool extensions make direct writes against Active Directory via LDAP and against policy files via a file access protocol. In policy application mode, CSEs use LDAP and a file access protocol to query the Group Policy server and the Group Policy file share data store, respectively, for the retrieval and application of policy settings.

Group Policy Server Communication Protocols

The Group Policy server uses the following communication protocols:

- LDAP, when accepting access to GPOs in Active Directory.
- File access protocol, for accepting local access to user and computer policy files, that is, when the Group Policy file share data store is located on the Group Policy server.

  Note that the core Group Policy engine on the Group Policy client chooses the appropriate protocol to invoke whenever the Group Policy client requires access to

Active Directory or the Group Policy file share. Likewise, the Administrative tool chooses the appropriate protocol to invoke when it needs access to Active Directory or the Group Policy file share.

Group Policy Data Store Communication Protocols

The Group Policy data store uses the following communication protocols:

- LDAP, when access is required for the storage and retrieval of GPOs in Active Directory.
- File access protocol, when access is required for updating and retrieving user and computer policy settings, and GPO version information, on the Group Policy file share.

The protocols and services that enable communications between Group Policy components are described as follows:

Authentication protocols: Authentication services, as described in [MS-AUTHSOD], are provided by NTLM, specified in [MS-NLMP], or Kerberos, as specified in [RFC4120] and [MS-KILE], to secure communications within the Group Policy protocols. These protocols also provides authentication services that support the client-to-server communication within and outside Group Policy. This includes the use of the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Protocol Extensions as described in [MS-SPNG], which facilitate a secure environment while negotiating which authentication protocol the Group Policy protocols use: either NTLM [MS-NLMP] or Kerberos [RFC4120], as described in [MS-SPNG], section 1.5.

DNS Server: DNS, as specified in [RFC1034] and [RFC1035], is used by both the Group Policy client and the Administrative tool to discover the location of the Group Policy server.

Internet Control Message Protocol (ICMP): In some instances, ICMP, as specified in [RFC792] is used by the Group Policy client to determine the network speed of the link to the domain controller, to ensure that bandwidth-intensive protocol extension sequences is sufficiently supported. See section 2.1.3.1.6 for more information on link speed determination.

Lightweight Directory Access Protocol: LDAP is invoked by the Group Policy: Core Protocol and may be invoked by Group Policy extensions to read and update various policy attributes stored in GPOs within the Active Directory hierarchy on the Group Policy server.

File access protocol: A file access protocol is invoked to read and update policy files on the Group Policy file share and to transmit policy settings and other data between the Group Policy server and Group Policy client.

2.1.2.2 Component Functionality

The following diagram shows the internal components and protocol connections for the Group Policy protocols.

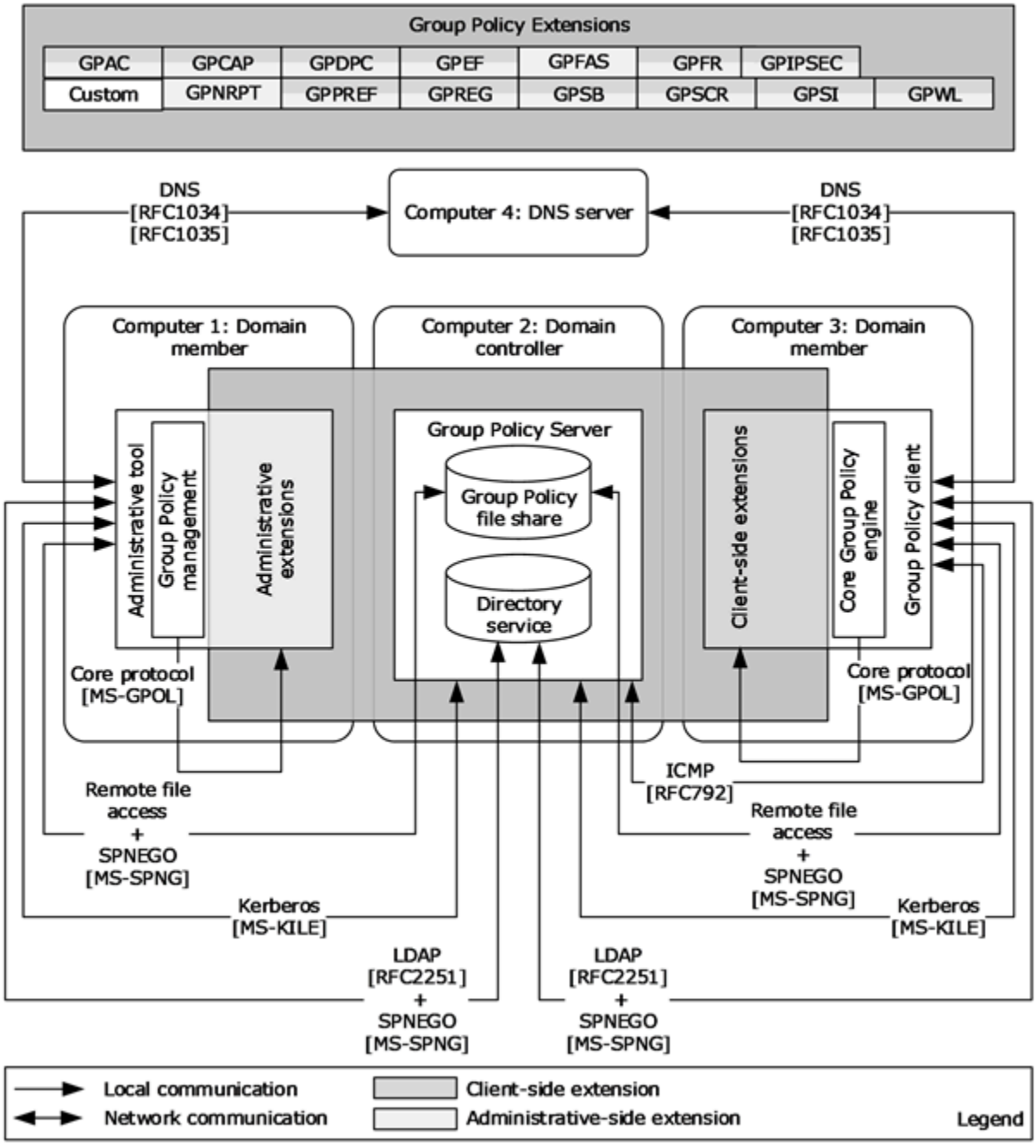


Figure 5: Internal component functions

The general functions of Group Policy components as follows:

Core Group Policy engine: Coordinates the application and processing of Group Policy by handling tasks such as:

- Applying Group Policy at regular intervals
- Accessing GPOs and retrieving GPO extension lists from Active Directory.
- Accessing policy settings on the Group Policy file share.
- Filtering and ordering GPOs
- Providing notification of Group Policy changes.

Extension protocols: Consist of CSE and Administrative tool extension protocols that extend Group Policy application functionality. Note that implementers can create their own custom extension protocols, as described in [MS-GPOL], section 1.8.

> In the preceding diagram, the color-code scheme indicates that most Group Policy extension protocols implement both an administrative-side and a client-side extension. However, the Group Policy: Firewall and Advanced Security Data Structure defined in [MS-GPFAS], implements only an administrative-side extension. For additional information about administrative-side and client-side extensions, see sections 1.1.4 and 2.2.

Group Policy file share: An implementation-specific version of a file share location. The Group Policy file share location and its internal directory structure are shared with all Group Policy clients and can be replicated to other peers in a multimaster topology.

Group Policy management: The Administrative tool provides facilities for locating, retrieving, creating, modifying, and deleting group policies. These management functions can be accomplished from an interface such as the GPMC, a custom application, or a command-line tool.

Directory service: An implementation-specific version of an LDAP-accessible directory service, such as Active Directory, for the storage of GPOs.

Group Policy Client-Side Extensions

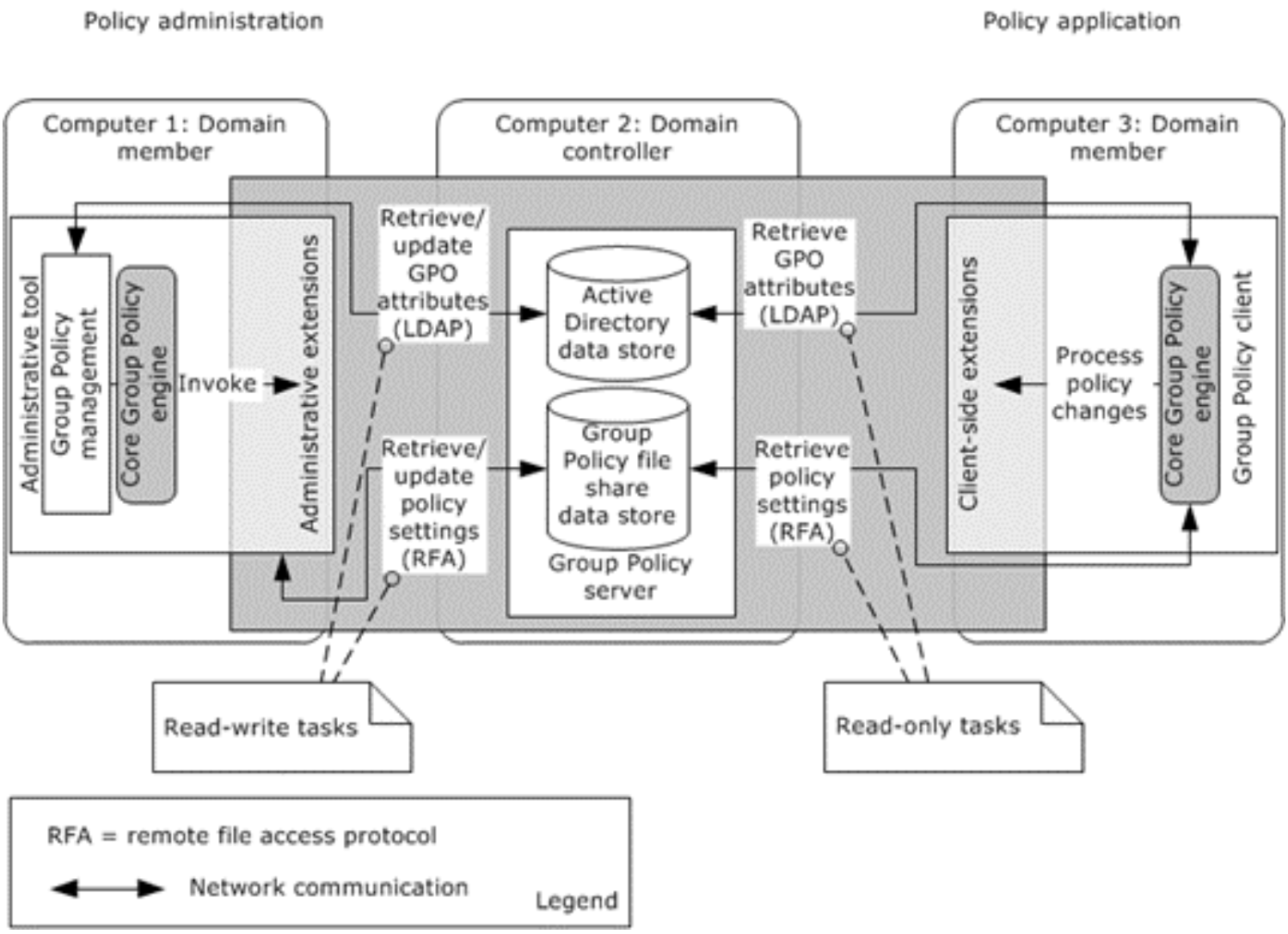
Client-Side Extension	CSE DLL	GUID
Wireless Group Policy	Wlgpclnt.dll	{0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63}
Group Policy Environment	Gpprefcl.dll	{0E28E245-9368-4853-AD84-6DA3BA35BB75}
Group Policy Local Users and Groups	Gpprefcl.dll	{17D89FEC-5C44-4972-B12D-241CAEF74509}
Group Policy Device Settings	Gpprefcl.dll	{1A6364EB-776B-4120-ADE1-B63A406A76B5}
Folder Restriction	Fdeploy.dll	{25537BA6-77A8-11D2-9B6C-0000F8080861}

Client-Side Extension	CSE DLL	GUID
Microsoft Disk Quota	Diskquota.dll	{3610eda5-77ef-11d2-8dc5-00c04fa31a66}
Group Policy Network Options	Gpprefcl.dll	{3A0DBA37-F8B2-4356-83DE-3E90BD5C261F}
QoS Packet Scheduler	Gptext.dll	{426031c0-0b47-4852-b0ca-ac3d37bfcb39}
Scripts	Gpscript.dll	{42B5FAAE-6536-11d2-AE5A-0000F87571E3}
Internet Explorer Zonemapping	Iedkcs32.dll	{4CFB60C1-FAA6-47f1-89AA-0B18730C9FD3}
Group Policy Drive Maps	Gpprefcl.dll	{5794DAFD-BE60-433f-88A2-1A31939AC01F}
Group Policy Folders	Gpprefcl.dll	{6232C319-91AC-4931-9385-E70C2B099F0E}
Group Policy Network Shares	Gpprefcl.dll	{6A4C88C6-C502-4f74-8F60-2CB23EDC24E2}
Group Policy Files	Gpprefcl.dll	{7150F9BF-48AD-4da4-A49C-29EF4A8369BA}
Group Policy Data Sources	Gpprefcl.dll	{728EE579-943C-4519-9EF7-AB56765798ED}
Group Policy Ini Files	Gpprefcl.dll	{74EE6C03-5363-4554-B161-627540339CAB}
Windows Search Group Policy Extension	Srchadmin.dll	{7933F41E-56F8-41d6-A31C-4148A711EE93}
Security	Scecli.dll	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Deployed Printer Connections	Gpprnext.dll	{8A28E2C5-8D06-49A4-A08C-632DAA493E17}
Group Policy Services	Gpprefcl.dll	{91FBB303-0CD5-4055-BF42-E512A681B325}
Internet Explorer Branding	Iedkcs32.dll	{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
Group Policy Folder Options	Gpprefcl.dll	{A3F3E39B-5D83-4940-B954-28315B82F0A8}
Group Policy Scheduled Tasks	Gpprefcl.dll	{AADCED64-746C-4633-A97C-D61349046527}
Group Policy Registry	Gpprefcl.dll	{B087BE9D-ED37-454f-AF9C-04291E351182}
EFS Recovery	Scecli.dll	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
802.3 Group Policy	Dot3gpclnt.dll	{B587E2B1-4D59-4e7e-AED9-22B9DF11D053}
Group Policy Printers	Gpprefcl.dll	{BC75B1ED-5833-4858-9BB8-CBF0B166DF9D}
Group Policy Shortcuts	Gpprefcl.dll	{C418DD9D-0D14-4efb-8FBF-CFE535C8FAC7}
Microsoft Offline Files	Cscobj.dll	{C631DF4C-088F-4156-B058-4375F0853CD8}
Software Installation	Appmgmts.dll	{c6dc5466-785a-11d2-84d0-00c04fb169f7}
IP Security	Polstore.dll	{e437bc1c-aa7d-11d2-a382-00c04f991e27}
Group Policy Internet Settings	Gpprefcl.dll	{E47248BA-94CC-49c4-BBB5-9EB7F05183D0}
Group Policy Start Menu Settings	Gpprefcl.dll	{E4F48E54-F38D-4884-BFB9-D4D2E5729C18}

Client-Side Extension	CSE DLL	GUID
Group Policy Regional Options	Gpprefcl.dll	{E5094040-C46C-4115-B030-04FB2E545B00}
Group Policy Power Options	Gpprefcl.dll	{E62688F0-25FD-4c90-BFF5-F508B9D2E31F}
Group Policy Applications	Gpprefcl.dll	{F9C77450-3A41-477E-9310-9ACD617BD9E3}
Enterprise QoS	Gptext.dll	{FB2CA36D-0B40-4307-821B-A13B252DE56C}

2.1.2.3 Component Tasks

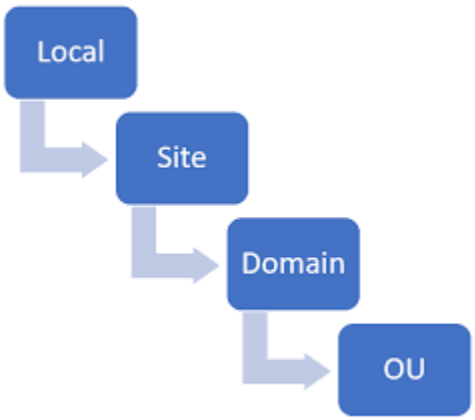
The following diagram provides a high-level depiction of the major tasks performed by Group Policy components. The sections following the diagram provide details about the messaging and Group Policy component functions that enable these tasks to be carried out.



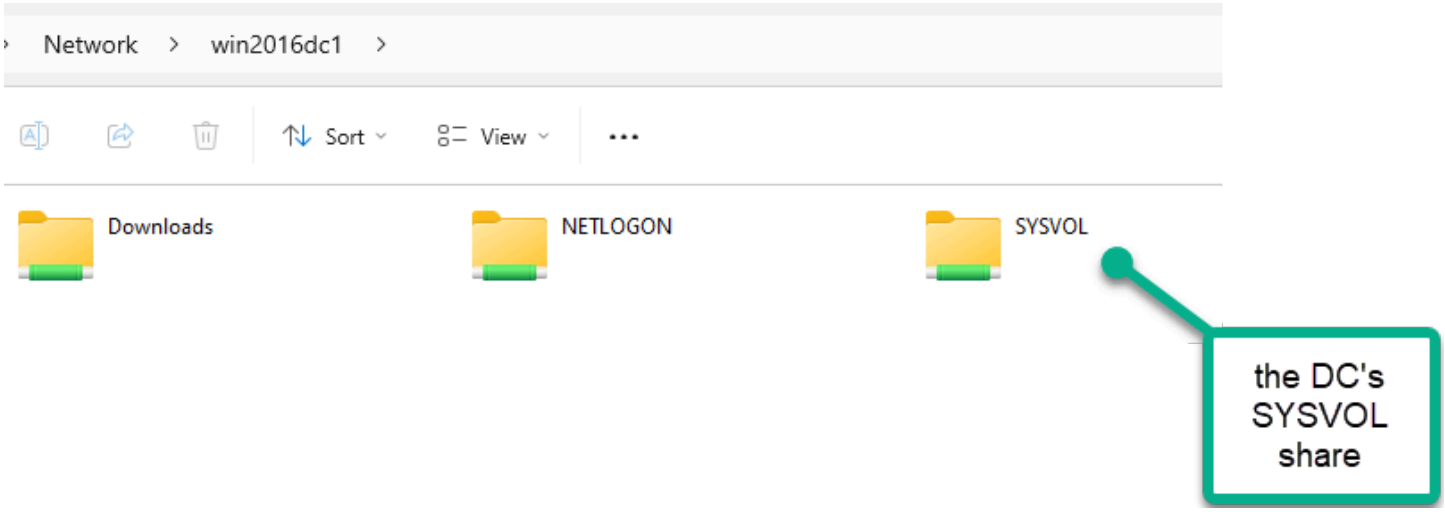
The technical relationship between Group Policy Objects (GPOs) and the Windows Registry

is fundamental in how GPOs apply configurations to computers and user accounts in a Windows environment. Here's an overview of this relationship:

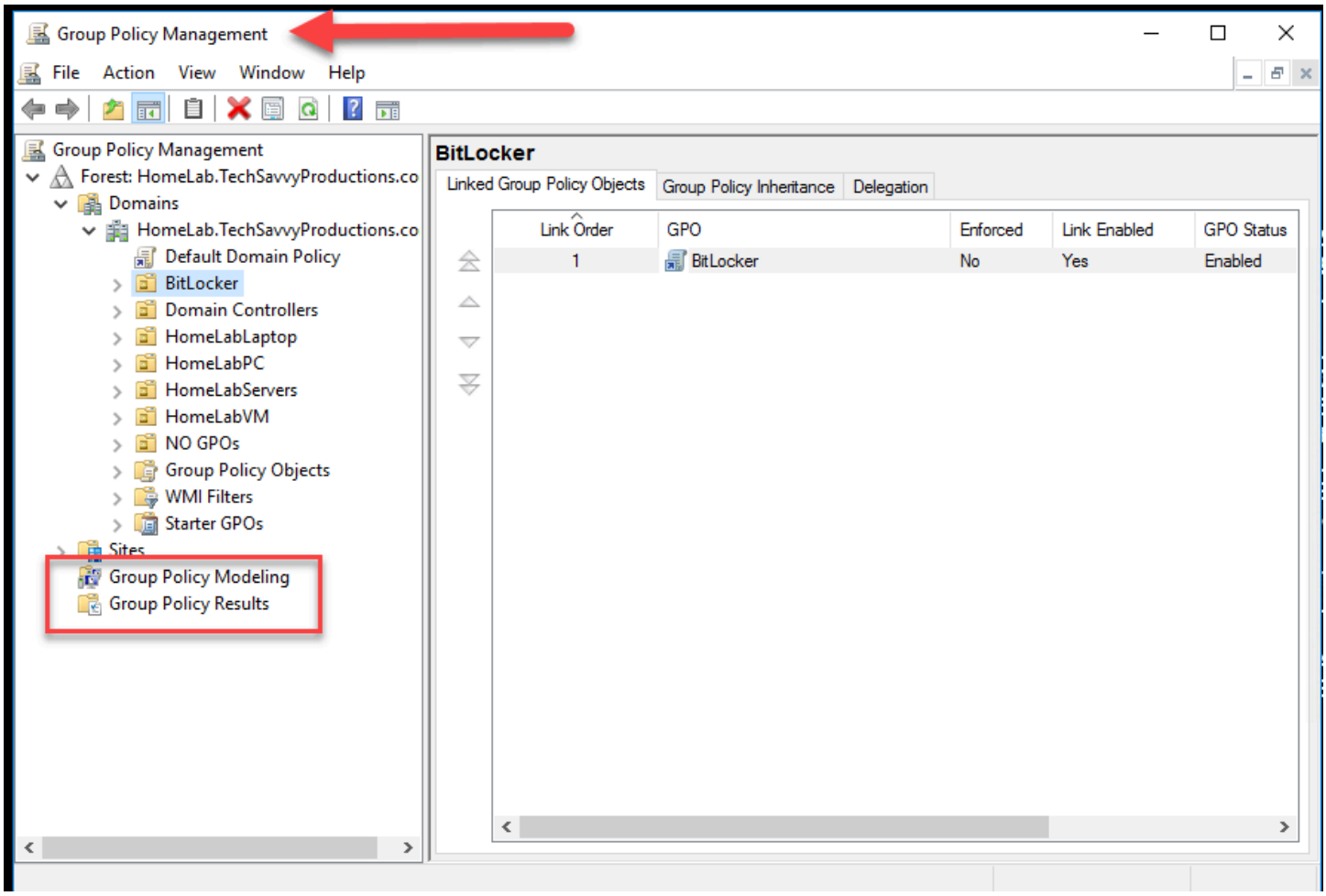
1. **Group Policy Settings and Registry Keys**: Many Group Policy settings directly correspond to specific registry keys and values. When a GPO is applied, it effectively sets or modifies certain registry keys on the target computer or user profile. For instance, a policy setting to change desktop background would modify a specific registry value that controls this aspect of the user interface.
2. **Policy vs. Preference**: In GPO, there are two types of settings: Policy settings and Preference settings. Policy settings are more enforceable and typically revert back to their original state when the policy is no longer applied. Preference settings, on the other hand, modify registry values but do not enforce them; the changes persist even after the policy is removed, unless explicitly configured otherwise.
3. **Registry.pol Files**: When Group Policy settings are applied, they are stored locally on the computer in Registry.pol files located in the C:\Windows\System32\GroupPolicy and C:\Windows\System32\GroupPolicyUsers directories. These files store policy settings that are applied to the computer and user registry hives, respectively.
4. **Processing GPOs and Updating the Registry**: When a computer starts up or a user logs in (as well as periodically while the system is running), the Group Policy engine processes GPOs linked to the computer and user accounts. It reads the settings from GPOs and applies them by updating the corresponding registry keys and values.
5. **Administrative Templates and Registry**: Administrative templates (.admx files) used in Group Policy Management provide a user-friendly interface to set policies. These templates actually map to specific registry keys and values. When an administrator configures a setting in an administrative template, they are indirectly configuring the associated registry entry.
6. **Group Policy and Registry Hierarchy**: The Group Policy engine processes policies in a specific order: local, site, domain, and then OU GPOs. This order ensures that policies applied at higher Active Directory levels can override local policies. The resulting registry changes reflect this hierarchy and precedence.



7. **Registry-Based Policy Settings**: Most of the settings under the "Administrative Templates" section in a GPO are registry-based settings. These settings are directly tied to specific registry paths and values.
8. **Central Store for Policy Definitions**: In an Active Directory environment, policy definitions are stored centrally in the domain's SYSVOL folder. These definitions help ensure consistency in how GPOs map to registry settings across different computers in the domain.



9. **GPO Tools Reflect Registry Settings**: Tools like the Resultant Set of Policy (RSoP) and Group Policy Results Wizard in the Group Policy Management Console can show the exact registry settings that are being applied by GPOs.



10. **Direct Registry Manipulation and GPO**: It's important to note that direct changes to the registry (not via GPO) can conflict with GPO settings. Such manual changes might be overwritten the next time GPOs are refreshed unless the corresponding policy is set to not configured.

Understanding this relationship is key to effectively managing Group Policy in a Windows environment, as it allows administrators to predict and understand how specific policies will affect the configuration of computers and user accounts.

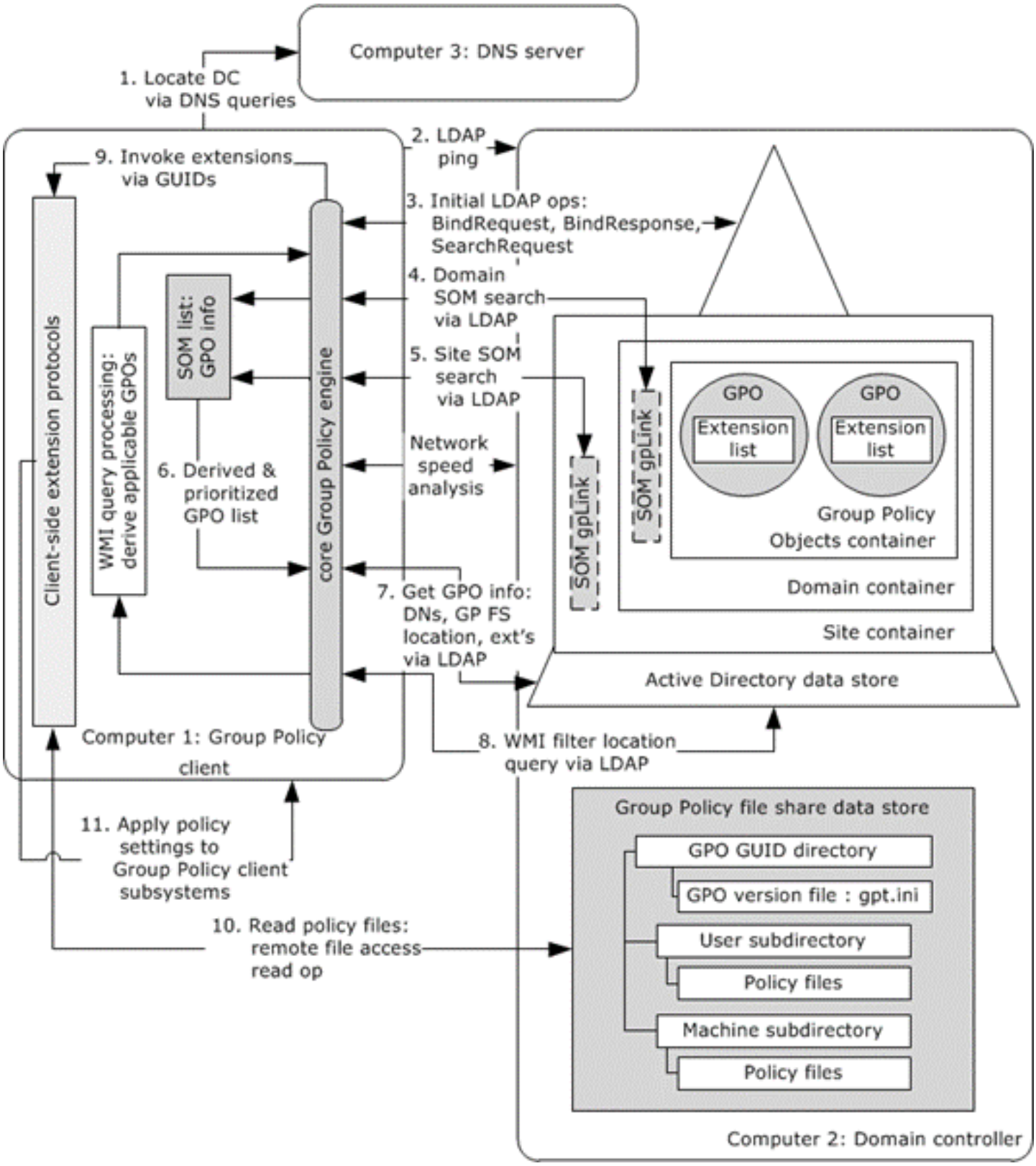
Not all Group Policy Objects (GPOs) in a Windows environment are fundamentally just registry edits

although many are closely related to registry settings. Group Policy is a broader framework that includes various types of settings and configurations, which can be categorized into two main groups:

1. **Registry-Based Policies**:
    - A significant portion of GPO settings, especially those found under "Administrative Templates," directly correspond to registry keys and values.
    - When these policies are applied, they modify specific registry entries on the target computer or user profiles.
    - These settings are typically used for configuring user environments, system settings, and application settings that are stored in the Windows Registry.
2. **Non-Registry-Based Policies**:
    - There are also GPO settings that do not directly translate to registry edits. These include:
        - **Scripts**: GPOs can be used to run logon, logoff, startup, and shutdown scripts. These scripts might not necessarily change registry settings but perform other actions.
        - **Folder Redirection**: This allows redirection of certain user folders (like Documents, Desktop) to network locations. While this might involve some registry changes, the primary function is managed through Group Policy without direct administrator interaction with the registry.
        - **Security Settings**: Some security settings, such as user rights assignments, security options, and advanced audit policy settings, are implemented through mechanisms other than direct registry edits.
        - **Software Installation and Maintenance**: GPOs can be used to deploy and manage software across a network, which involves more than just registry modifications.
        - **Group Policy Preferences**: This includes settings like drive mappings, printer connections, and file settings, which often go beyond simple registry configurations.

In summary, while many GPO settings are indeed registry edits at their core, Group Policy as a whole encompasses a wider range of system management capabilities. Some of these capabilities involve registry changes, while others are managed through different mechanisms within the Windows operating system.

Implementing Active Directory (AD) Group Policy Objects (GPOs) involves various protocols and services within a Windows network environment.



The major protocols and services used are:

1. **LDAP (Lightweight Directory Access Protocol)**: LDAP is used for accessing and modifying directory services, such as Active Directory, over an IP network. It plays a crucial role in querying AD for GPO information.

2. **Kerberos**: Kerberos is used for authentication in a Windows network. It ensures that users and computers in an AD domain are authenticated before GPOs are applied.
3. **SMB (Server Message Block)**: SMB is used for file sharing, including the distribution of GPO files. When a GPO is processed, the client machine retrieves the GPO files (like scripts, templates, and ADMX files) from a shared folder, typically stored on a domain controller, using the SMB protocol.
4. **DNS (Domain Name System)**: DNS is essential for locating domain controllers within an AD domain. It ensures that client machines can find the appropriate domain controller to retrieve GPOs.
5. **RPC (Remote Procedure Call)**: RPC is used for inter-process communication. It enables the Group Policy client on a Windows machine to communicate with the Group Policy engine on a domain controller to retrieve and apply GPOs.
6. **NTLM (NT LAN Manager)**: In cases where Kerberos is not used, NTLM might be used as a fallback for authentication between clients and servers within an AD environment.
7. **HTTP/HTTPS**: In some configurations, especially involving centralized management or cloud integration, Group Policy settings might be retrieved over HTTP/HTTPS protocols.
8. **Sysvol Replication Protocols (FRS or DFSR)**: File Replication Service (FRS) or Distributed File System Replication (DFSR) are used for replicating the Sysvol folder across domain controllers. The Sysvol folder contains Group Policy template files, making its replication crucial for consistent GPO application across the domain.
9. **Group Policy Caching (Offline Files)**: This uses the Offline Files feature, which operates over the SMB protocol, to cache GPOs locally on client machines for faster processing.
10. **WMI (Windows Management Instrumentation)**: While not a protocol, WMI is used extensively in Group Policy for applying settings conditionally using WMI filters. It allows querying of a wide range of system properties.

These protocols and services work together to ensure that GPOs are effectively distributed, applied, and managed across a Windows network, maintaining the security, efficiency, and consistency of policy enforcement.

LDAP (Lightweight Directory Access Protocol) plays a significant role in the functioning of Group Policy Objects (GPOs) in a Windows Active Directory (AD) environment.

Here's what LDAP does in regards to GPOs:

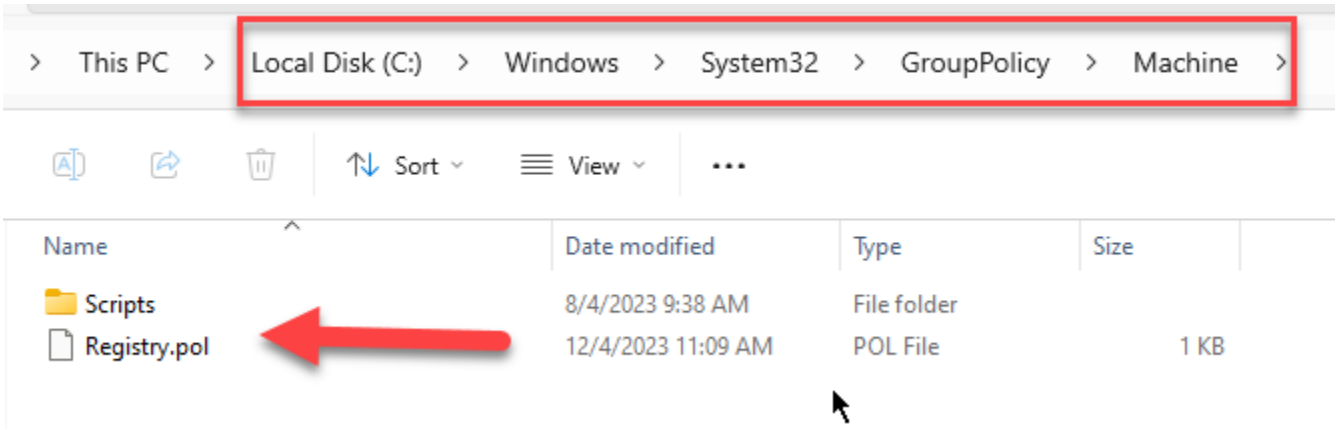
1. **GPO Retrieval**: LDAP is used to query Active Directory for the GPOs that are applicable to a specific user or computer. When a user logs in or a computer starts up, the Group Policy client uses LDAP to determine which GPOs should be applied based on the user's or computer's AD object and group memberships.
2. **Accessing GPO Information**: GPOs are stored in Active Directory. LDAP is used to access the GPO information, such as the list of GPOs linked to an Organizational Unit (OU), the GPOs' order of application, and any security filtering or WMI filtering settings.
3. **Reading GPO Attributes**: LDAP is used to read various attributes of a GPO stored in Active Directory. These attributes include the GPO's unique ID (GUID), version number, and the path to the GPO's content in the Sysvol folder on a domain controller.
4. **Access Control**: LDAP is involved in checking access control lists (ACLs) for GPOs. This determines whether the user or computer has the necessary permissions to read and apply a given GPO.
5. **Facilitates GPO Processing**: In the background, LDAP queries help the Group Policy client to process GPOs correctly. This includes determining which GPOs are new or have changed, which need to be downloaded from the domain controller, and which are no longer applicable and should be unapplied.
6. **WMI Filtering**: When a GPO has an associated WMI filter, LDAP is used to retrieve this filter from AD. The Group Policy client then evaluates this filter to determine if the GPO should be applied.
7. **Site-Based GPO Application**: For GPOs linked to an AD site, LDAP queries are used to determine the site to which a computer belongs, which then influences which GPOs are applicable to that computer.

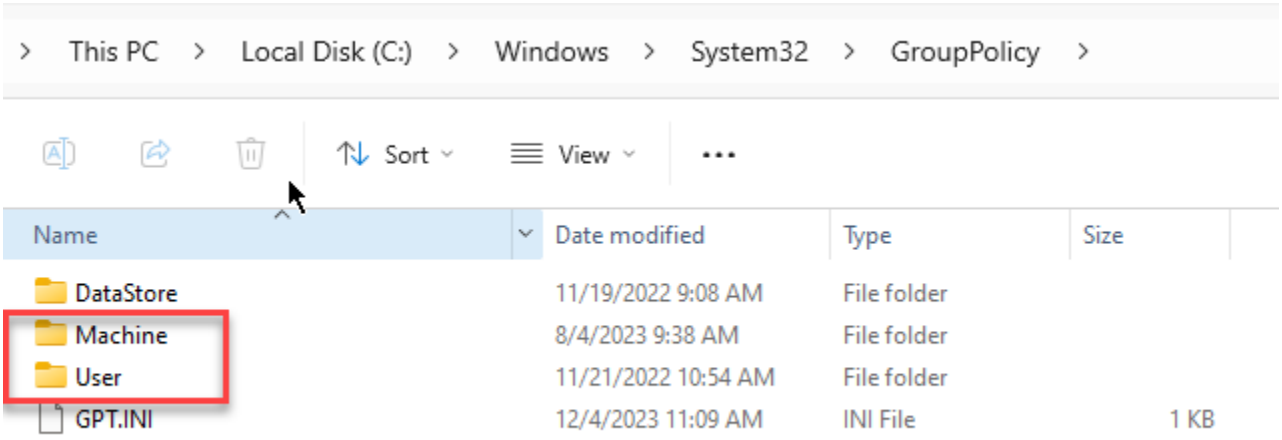
In summary, LDAP acts as a communication protocol allowing Group Policy clients (on user computers) to interact with Active Directory for retrieving and understanding GPO information. This interaction is crucial for the correct application of GPOs in an AD environment.

The Group Policy engine in Windows clients,

responsible for processing and applying Group Policy settings, relies on several key components and files. While the exact implementation can vary slightly between different versions of Windows, the core components typically include:

1. **Group Policy Client Service (gpsvc.dll)**: This is a Windows service that is responsible for applying Group Policy settings. It runs in the background and ensures policies are applied correctly, both at logon and at regular intervals while the system is running.
2. **Local Group Policy Database (Registry.pol)**: These files, found in C:\Windows\System32\GroupPolicy\Machine and C:\Windows\System32\GroupPolicy\User, store the local Group Policy settings applied to the computer and current user, respectively. They are essentially registry policy files that store registry-based policy settings.

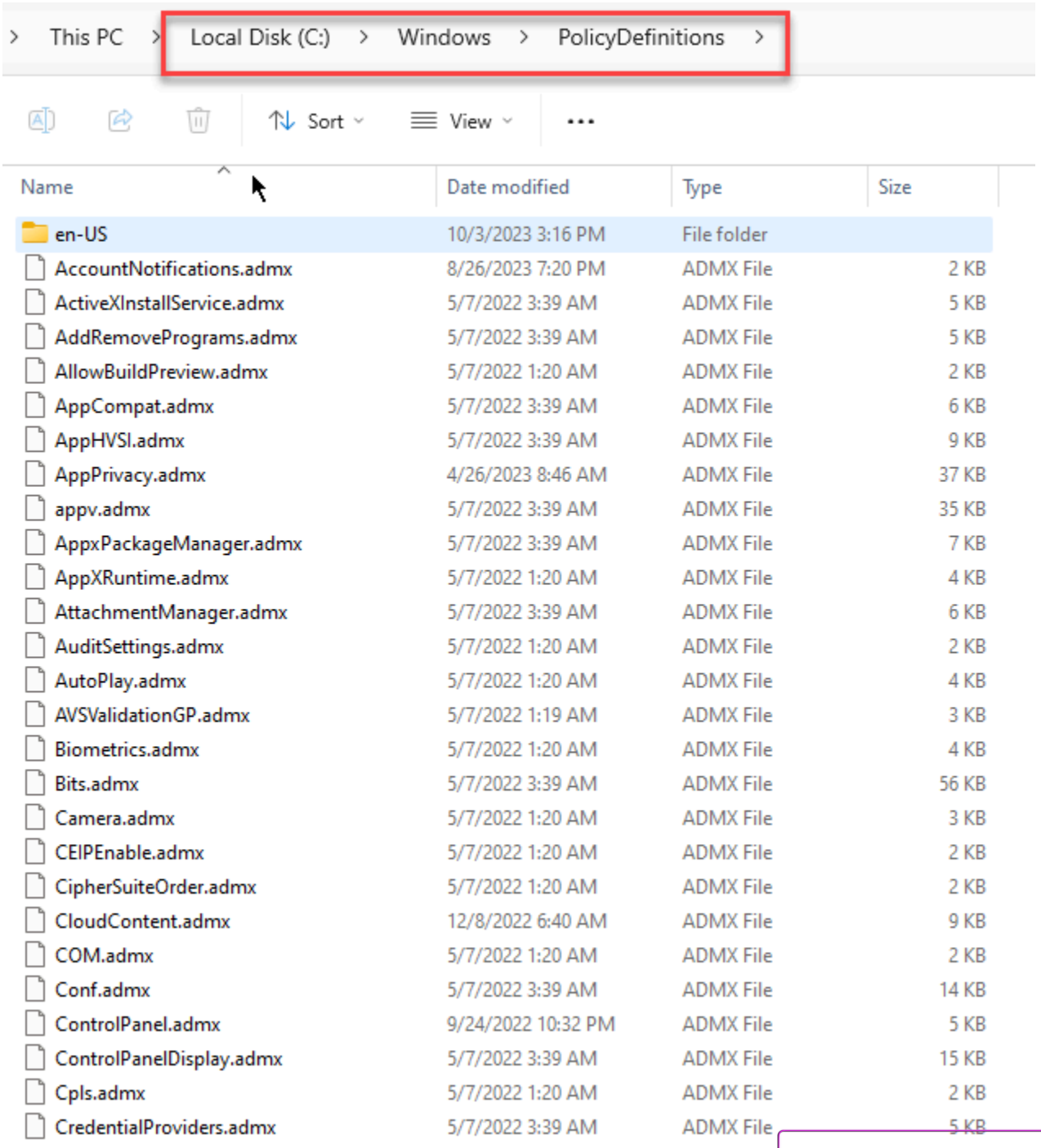




3. **Group Policy CSEs (Client Side Extensions)**: These are DLL files that extend the Group Policy client with additional capabilities to process specific types of policy settings. Examples include:
    - **gptext.dll**: For processing scripts policies.

- **fdeploy.dll**: For Folder Redirection.
- **iedkcs32.dll**: For Internet Explorer maintenance.
- **wmicmiplugin.dll**: For WMI filters.

4. **Administrative Templates (ADMX/ADML Files)**: These XML-based files, located in C:\Windows\PolicyDefinitions (for central store) or within the local machine, define the available settings within Group Policy Administrative Templates. They are used to generate the user interface for policy configuration in the Group Policy Management Editor.



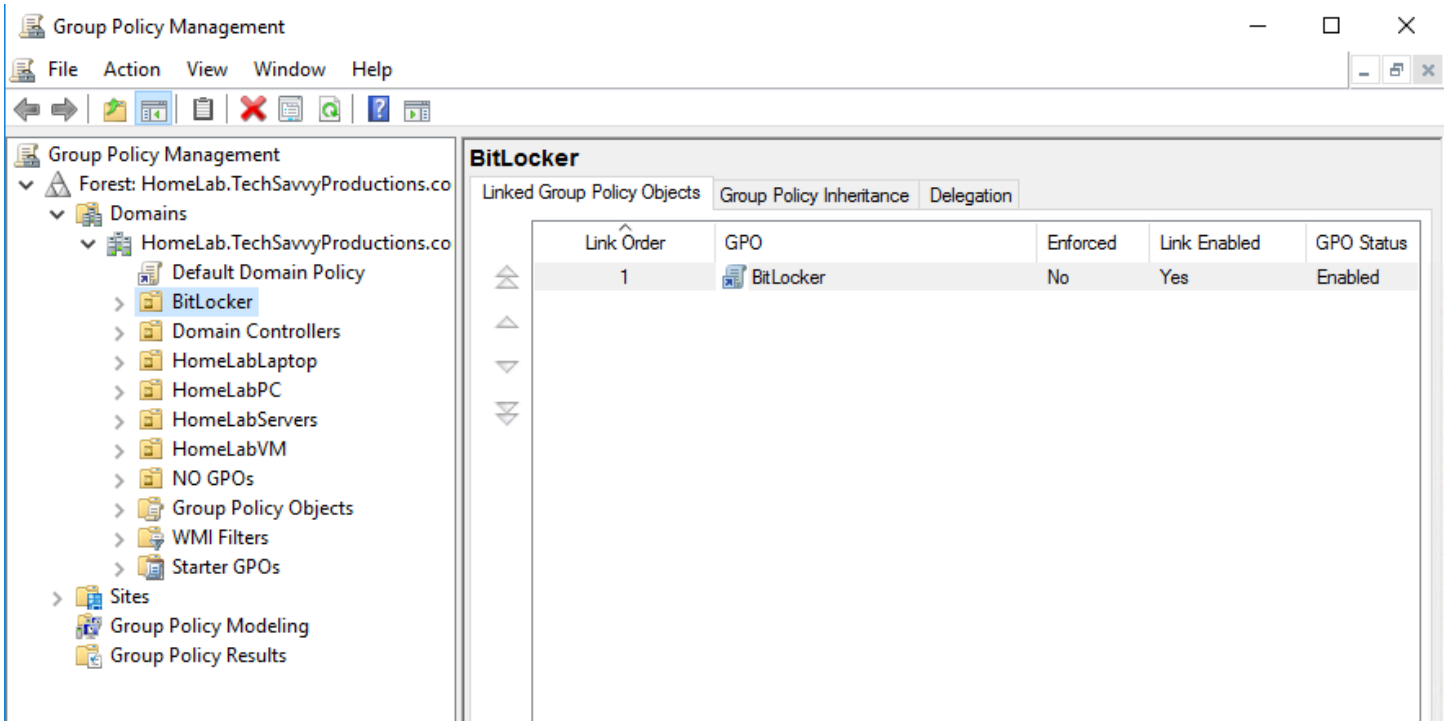
5. **Group Policy Template Files (GPT)**: These are stored in the SYSVOL share on domain controllers and are replicated to all domain controllers in the domain. They contain the actual policy settings and scripts that are applied to users and computers in the domain.
6. **gpmc.msc (Group Policy Management Console)**: Although not part of the client's Group Policy processing engine, GPMC is the management tool used to create and manage Group Policies in a domain environment.
7. **secedit.exe**: This command-line tool is used for configuring and analyzing system security by enforcing security policies.
8. **gpresult.exe and rsop.msc (Resultant Set of Policy)**: These tools are used for troubleshooting and reporting on Group Policy settings applied to a particular user or computer.
9. **gpupdate.exe**: A command-line tool used to manually force a Group Policy update on a local machine.

These components work together to ensure that Group Policy settings are processed, applied, and maintained as defined by the network administrators. The Group Policy engine is a complex system that integrates deeply with various aspects of the Windows operating system, ensuring that policies are enforced in a consistent and reliable manner.

On a Windows Domain Controller, several components work together to support the functions of Group Policy Objects (GPOs).

These components are essential for the creation, management, storage, and dissemination of GPOs across the Active Directory (AD) environment:

1. **Active Directory Database**: The AD database stores information about all GPOs created in the domain. This includes the GPO's properties, such as its unique identifier (GUID), security filtering settings, WMI filter links, and more.
2. **SYSVOL Share**: The SYSVOL folder on each domain controller contains the Group Policy Template (GPT), which includes the actual policy settings, scripts, and other files that are part of the GPO. SYSVOL replication ensures that these files are consistent across all domain controllers.
3. **Group Policy Management Console (GPMC)**: This is a management tool used by administrators to create, edit, link, and manage GPOs. It provides a user interface for interacting with GPOs stored in Active Directory and the SYSVOL share.



4. **Group Policy Engine**: This engine on the domain controller processes GPO-related tasks, such as generating resultant sets of policy (RSoP) data and responding to client-side requests for GPO information.

5. **LDAP Service**: The Lightweight Directory Access Protocol (LDAP) service is used to query the Active Directory database for GPOs applicable to a specific user or computer.
6. **Kerberos and NTLM**: These authentication protocols are used to authenticate clients that request GPOs and to secure the communication between clients and the domain controller.
7. **File Replication Service (FRS) or Distributed File System Replication (DFSR)**: These services are responsible for replicating the contents of the SYSVOL share among all domain controllers in a domain. DFSR is used in more recent versions of Windows Server, replacing FRS.
8. **DNS Service**: The Domain Name System (DNS) service is critical for clients to locate domain controllers for GPO processing and for domain controllers to communicate within an AD forest.
9. **Windows Management Instrumentation (WMI)**: WMI filters in GPOs allow administrators to apply policies conditionally based on various criteria. The WMI service on domain controllers is used to evaluate these filters.
10. **Group Policy Client Service on DC**: This service, also running on domain controllers, processes GPOs for the domain controller itself, ensuring that policies applicable to domain controllers are enforced.

These components collectively ensure that GPOs are effectively managed, replicated, and applied across the entire Active Directory environment, enabling centralized configuration and management of networked computers and user settings.

Understanding Group Policy in Windows environments

especially its advanced settings, involves several key concepts. Here are ten important concepts to grasp:

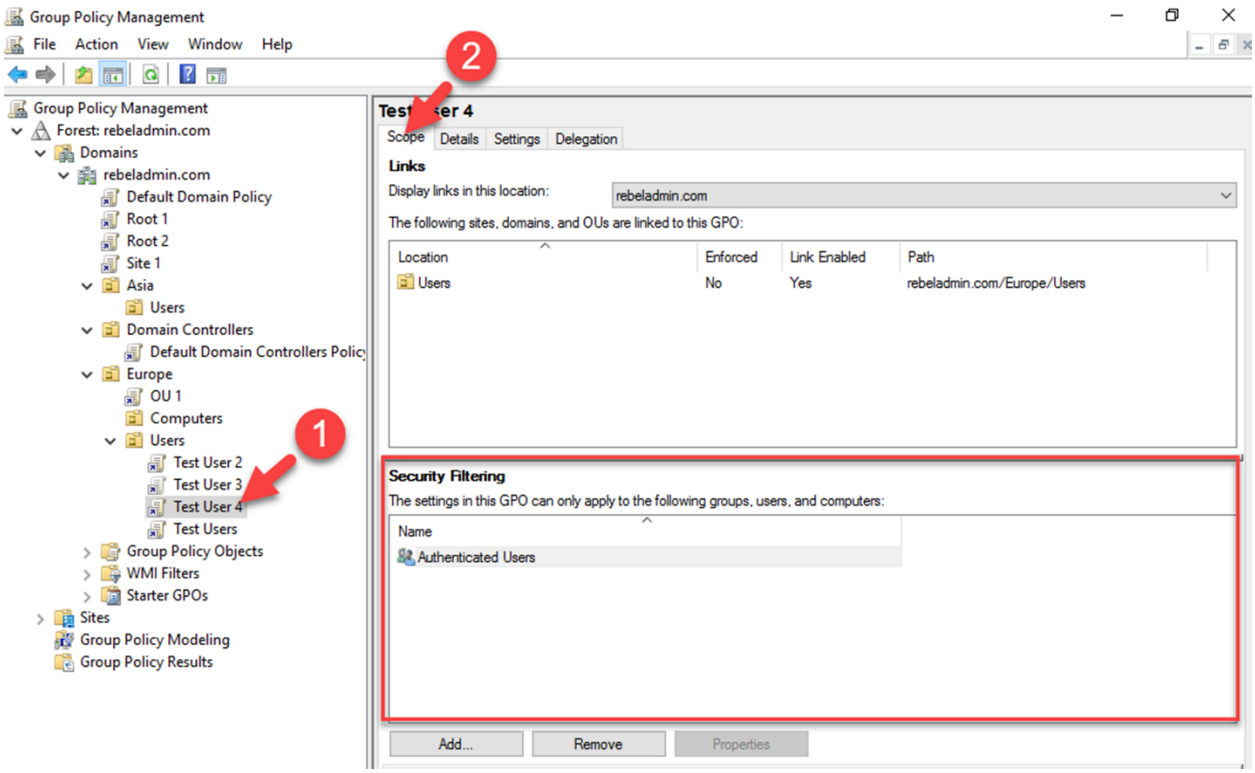
1. **Group Policy Objects (GPOs)**: These are the core elements of Group Policy, which administrators use to define configurations for users and computers within an Active Directory environment.
2. **Organizational Units (OUs)**: These containers in Active Directory can be used to group users or computers on which specific GPOs are applied. Understanding how to structure OUs effectively is crucial for managing and applying GPOs.
3. **Inheritance and Precedence**: GPOs can be linked to multiple levels in the Active Directory hierarchy (site, domain, OU). GPOs linked to lower levels in the hierarchy have precedence, but settings can also be inherited from higher levels.
4. **Enforced (No Override) Setting**: This setting can be applied to GPOs to prevent them from being overridden by other GPOs. It's an essential concept in complex Group Policy environments.
5. **WMI Filters**: Windows Management Instrumentation (WMI) filters allow administrators to apply GPOs based on attributes of the target computers or users, such as operating system version or hardware configuration.
6. **Security Filtering**: This allows administrators to control which users or groups a GPO applies to. It can be used to apply policies selectively within a broader scope (like an OU).
7. **Loopback Processing**: In certain scenarios, such as on terminal servers, you might want user policies to be determined by the computer they're logging onto rather than their user object in Active Directory. Loopback processing enables this functionality.
8. **Item-Level Targeting**: This feature in Group Policy Preferences allows you to apply settings based on specific attributes of the target object, like IP range, computer name, network status, etc.
9. **Group Policy Modeling and Resultant Set of Policy (RSoP)**: These tools help in planning (Group Policy Modeling) and troubleshooting (RSoP) Group Policy implementations by showing what policies would or have been applied to users and computers.
10. **Advanced Delegation**: Understanding how to delegate control of GPOs, such as allowing specific users to edit or manage certain GPOs without giving them broader administrative privileges, is essential for larger or more segmented environments.

in complex Active Directory environments. Mastery of these areas enables administrators to leverage Group Policy for robust and granular management of user and computer settings across a network.

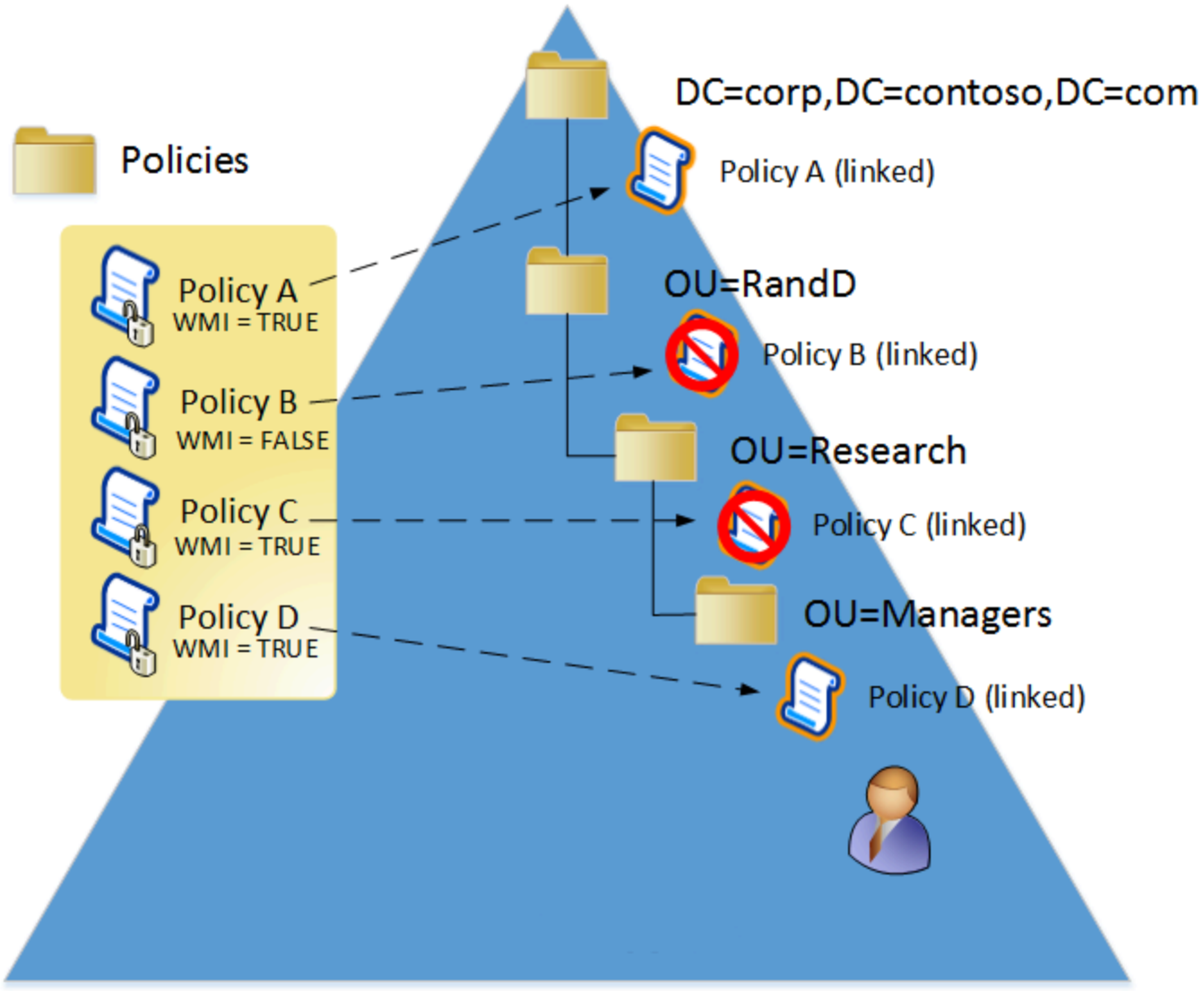
Understanding and implementing Group Policy in a Windows environment requires familiarity with several key concepts:

1. **Group Policy Object (GPO)**: A GPO is a collection of policy settings created using the Group Policy Management Console (GPMC). These policies control the behavior of users and computers in an Active Directory environment.
2. **Organizational Units (OUs)**: OUs are containers in Active Directory where users, groups, and computers are organized. GPOs can be linked to OUs to apply specific policies to the objects within them.
3. **Inheritance and Precedence**: GPOs can be linked at various levels in the Active Directory hierarchy, such as:
    I. site,
    II. domain,
    III. and OU.
    IV. Policies applied at lower levels can override those at higher levels, unless inheritance is blocked or settings are enforced.

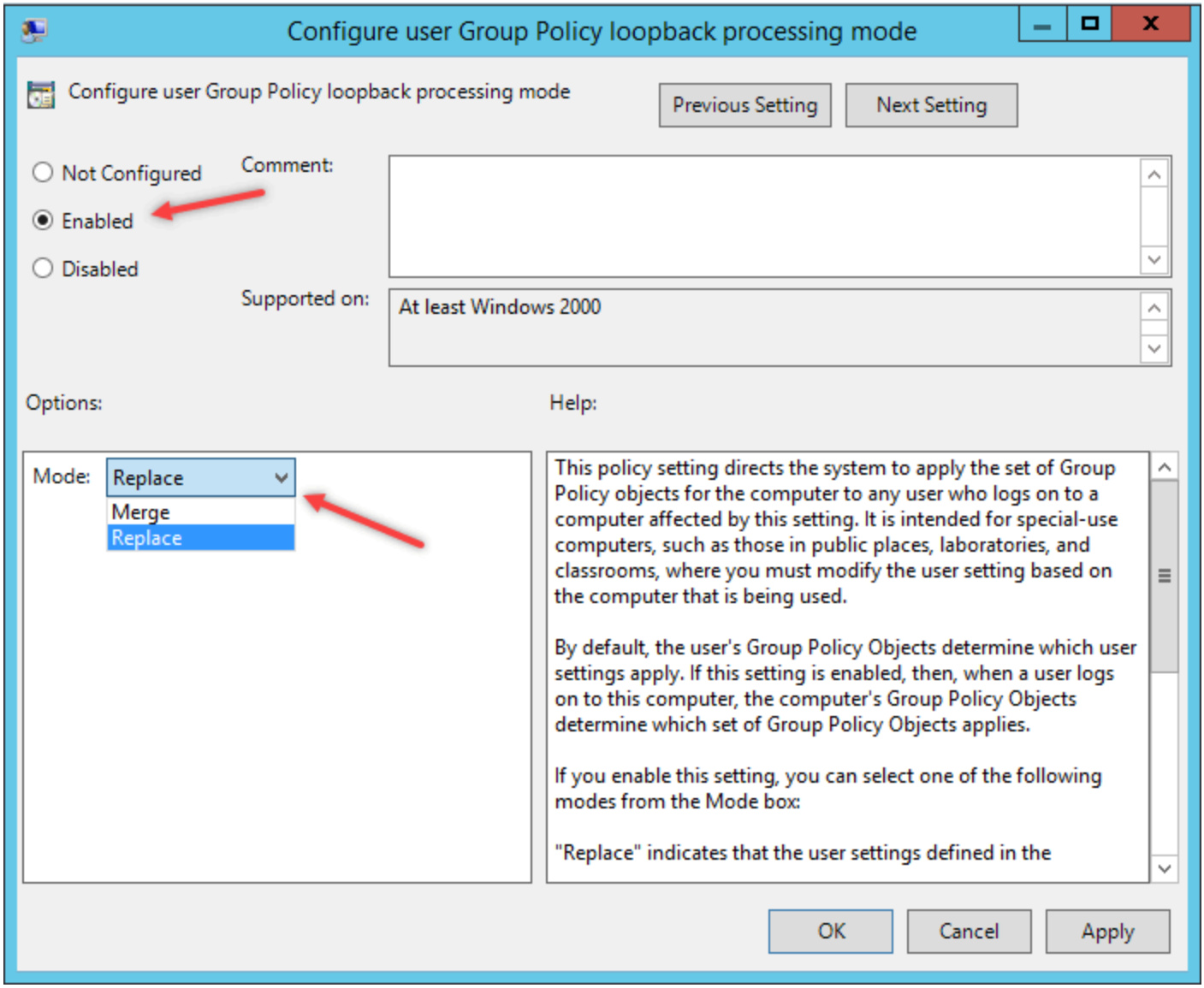
4. **Security Filtering**: This allows you to apply GPOs to specific users or groups within an OU, providing a way to fine-tune policy application based on security group membership.

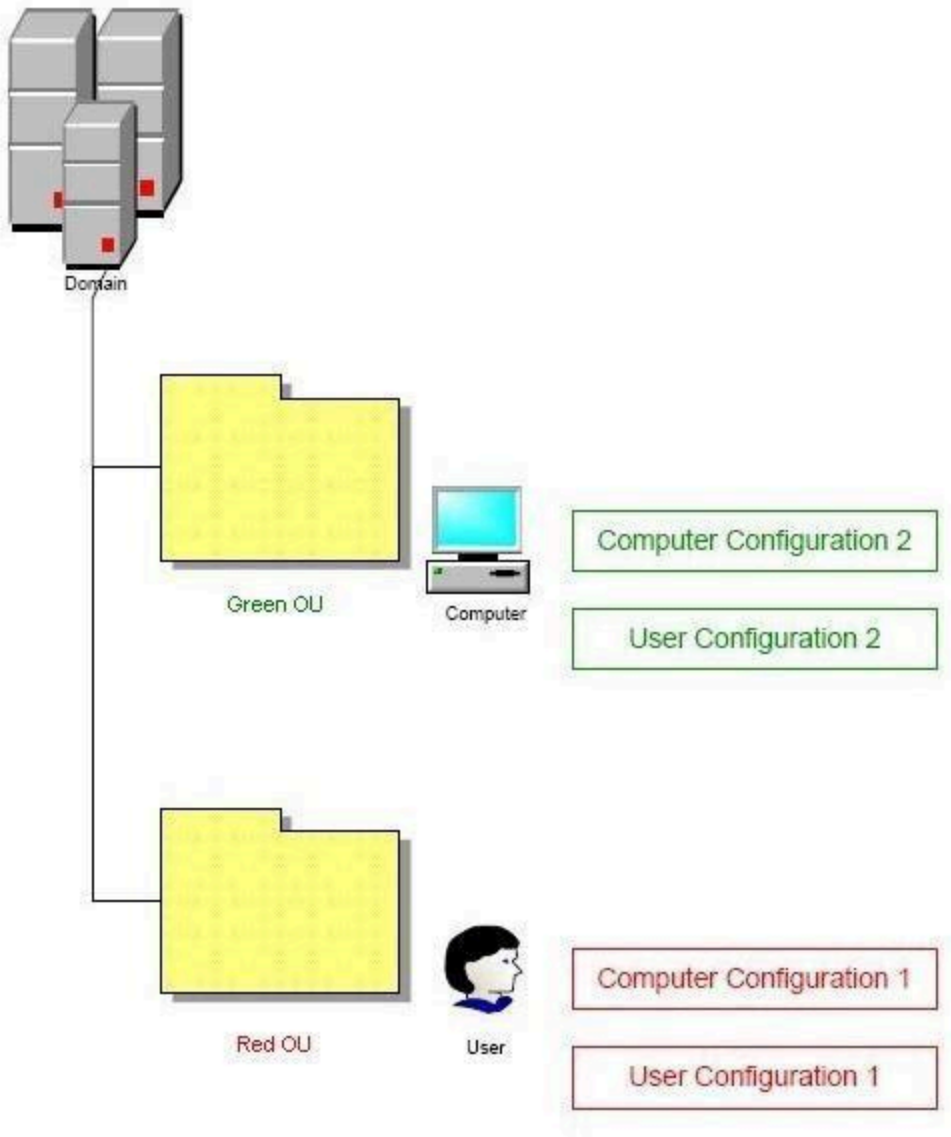


5. **WMI Filters**: Windows Management Instrumentation (WMI) filters enable the application of GPOs based on attributes of the target computer, such as operating system version or hardware specifications.



6. **Loopback Processing**: This feature changes the way GPOs are processed. Normally, user policies are applied based on the user's location in Active Directory. With loopback processing, user policies can be applied based on the computer's location, useful in shared computer scenarios.





7. **Link-Enabled and Link-Order**: GPOs must be linked to an Active Directory site, domain, or OU to be effective. The link order determines the order in which GPOs are applied when multiple GPOs are linked to a single container.
8. **Enforced Policies**: GPOs marked as "Enforced" have their settings applied even if conflicting policies are set at a lower level. This is useful for applying critical security settings or other important configurations.
9. **Group Policy Refresh**: Group Policy settings are periodically refreshed in the background for both user and computer configurations. Understanding and potentially modifying refresh intervals can be important for policy management.
10. **Group Policy Results Tool and Group Policy Modeling**: These tools in the GPMC allow administrators to troubleshoot GPO application issues (Results Tool) and predict the impact of GPO changes before they are applied (Modeling).

A thorough understanding of these concepts is crucial for effectively leveraging Group Policy in a Windows environment, enabling administrators to manage system settings and user experiences efficiently across an organization.

Troubleshooting Group Policy Objects (GPOs)

in a Windows environment can be complex, but there are fundamental steps you can follow to identify and resolve issues:

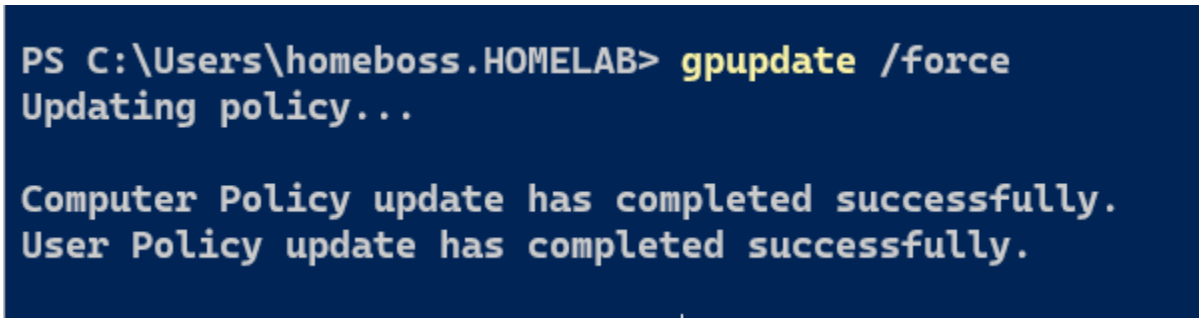
1. **Verify GPO Linking**: Ensure that the GPO is properly linked to the correct Organizational Unit (OU), domain, or site where the target users or computers reside.
2. **Check Group Policy Inheritance**: Examine the order and level at which GPOs are applied, considering inheritance and any enforced policies that could override your settings.
3. **Review Security Filtering**: Confirm that the appropriate security groups are included in the Security Filtering section of the GPO, allowing the policy to be applied to the intended users or computers.
4. **Examine WMI Filters**: If a WMI filter is applied to the GPO, ensure that the filter criteria are correct and relevant for the target computers or users.
5. **Evaluate GPO Settings**: Go through the specific settings within the GPO to ensure they are configured correctly and do not conflict with other settings.
6. **Use Group Policy Results Wizard**: Run the Group Policy Results Wizard in the Group Policy Management Console (GPMC) on the affected user and computer to get a report of all policies being applied and to identify any errors.
7. **Check Replication**: Ensure that Group Policy changes have replicated to all domain controllers in the environment. Replication issues can cause inconsistencies in GPO application.
8. **Inspect Event Logs**: Look at the Event Viewer on the affected client machines and domain controllers for any Group Policy-related errors or warnings.
9. **Use Command-Line Tools**: Utilize command-line tools like gpresult /r for a quick overview of applied policies on a client machine, or gpupdate /force to force a Group Policy update.
10. **Loopback Processing Mode**: If user settings are not applying correctly, check if the Loopback Processing mode is enabled, which can cause user policies to be applied based on the computer's location in the AD instead of the user's.
11. **Network Connectivity and Permissions**: Ensure there are no network connectivity issues between the client machines and the domain controllers, and verify that the user and computer accounts have the necessary permissions to read the GPO.
12. **Consult Documentation and Community**: If the issue persists, consult Microsoft's documentation, and community forums, or consider reaching out to Microsoft Support for more in-depth troubleshooting.

By following these steps methodically, you can identify and resolve most issues related to GPO application in a Windows environment.

gpupdate is a command-line tool used to refresh Group Policy settings immediately

rather than waiting for the next periodic update. This tool can be very helpful in troubleshooting GPO related problems. Here's how to use gpupdate effectively:

1. **Open Command Prompt**: Start by running Command Prompt as an administrator. This ensures that you have the necessary permissions to apply all Group Policy settings.
2. **Basic Usage**: The simplest form of the command is gpupdate, which refreshes both user and computer Group Policy settings. This command applies any new or changed policies since the last refresh.
3. **Update Computer Policies Only**: If you want to update only the computer policies and not the user policies, use gpupdate /target:computer. This is useful when you know the change is related to computer configuration.
4. **Update User Policies Only**: Similarly, use gpupdate /target:user to refresh only user policies. This is helpful when the change is related to user configuration.
5. **Force Update**: To ensure that all policies are reapplied, not just the new or changed ones, use gpupdate /force. This command re-applies all policy settings, which can help resolve issues where the policy might not have been applied correctly.



6. **Wait for Policy Processing**: By default, gpupdate runs asynchronously. To make the command prompt wait until the Group Policy processing is finished, use the /wait switch, like gpupdate /wait:30 to wait for 30 seconds. Adjust the time as needed.
7. **Logoff After Updating User Policies**: Some user policy changes (like software installation) require a logoff to take effect. Use gpupdate /logoff to automatically log off the user after the refresh if such policies need to be applied.
8. **Restart After Updating Computer Policies**: Similarly, if the computer policy requires a restart (like computer startup scripts), use gpupdate /boot to automatically restart the computer after the policy refresh.

9. **Check Command Output**: After running gpupdate, check the command output for any errors or messages indicating that policies have been updated or if additional actions (like logoff or restart) are required.
10. **Troubleshoot Remote Computer**: gpupdate is generally used for the local machine. For remote machines, you would typically use tools like Group Policy Management Console (GPMC) or PowerShell scripts to trigger a Group Policy update remotely.

By using gpupdate in various scenarios as outlined, you can effectively force the application of new or changed Group Policy settings, which is a key step in troubleshooting GPO-related problems.

Using the gpresult command is an effective way to troubleshoot Group Policy Object (GPO)

related issues in a Windows environment. Here's how you can utilize gpresult for troubleshooting:

1. **Open Command Prompt**: Run Command Prompt as an administrator. This is important for ensuring that you have sufficient permissions to view all GPO-related information.
2. **Basic Usage**: To quickly view the applied GPOs for the current user and computer, type gpresult /R. This command provides a summary of the last time Group Policy was applied, the domain controller which applied it, and the list of applied GPOs for the user and the computer.

```
PS C:\Users\homeboss.HOMELAB> gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on 12/5/2023 at 3:16:03 PM


RSOP data for HOMELAB\HomeBoss on AMDVE : Logging Mode
-----------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.22621
Site Name:                   HQ-Homelab
Roaming Profile:             N/A
Local Profile:               C:\Users\homeboss.HOMELAB
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=AMDVE,OU=HomeLabPC,DC=HomeLab,DC=TechSavvyProductions,DC=com
    Last time Group Policy was applied: 12/5/2023 at 3:14:41 PM
    Group Policy was applied from:      Win2016DC1.HomeLab.TechSavvyProductions.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        HOMELAB
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        Enable WinRM
        Windows Update
        Disable Anonymous SID Enumeration
        Disable Guest Account
        Storing LAN Manager Hash
        PowerShell Execution Policy
        Security Audits
        Remote Event Viewer Firewall GPO
        Default Domain Policy
```

Local Group Policy

The computer is a part of the following security groups

BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
AMDVE$
Domain Computers
Authentication authority asserted identity
System Mandatory Level

USER SETTINGS

CN=HomeBoss,CN=Users,DC=HomeLab,DC=TechSavvyProductions,DC=com
Last time Group Policy was applied: 12/5/2023 at 3:14:42 PM
Group Policy was applied from: Win2016DC1.HomeLab.TechSavvyProductions.com
Group Policy slow link threshold: 500 kbps
Domain Name: HOMELAB
Domain Type: Windows 2008 or later

Applied Group Policy Objects

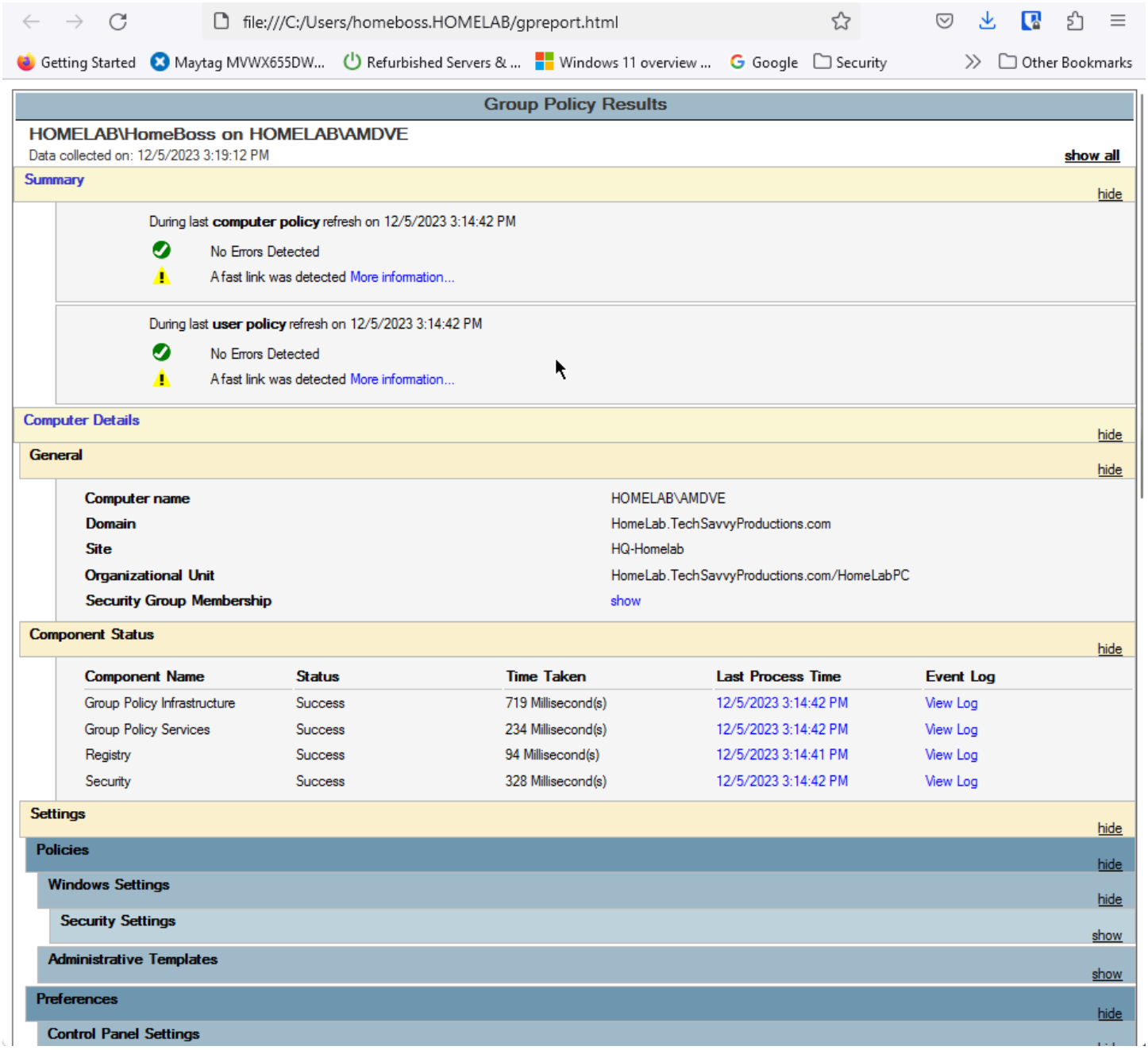
N/A

The following GPOs were not applied because they were filtered out
---
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups

Domain Users
Everyone
BUILTIN\Users
BUILTIN\Administrators
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Domain Admins
Authentication authority asserted identity
Denied RODC Password Replication Group
High Mandatory Level

3. **View Detailed Report**: For a more detailed report, **`use gpresult /H GPReport.html`** to generate an HTML file named "GPReport.html" with detailed GPO information. This file will be saved in the directory where the command is run.



4. **Check for a Specific User**: To run gpresult for a specific user, use the /USER parameter, like gpresult /R /USER [username]. Replace [username] with the actual username.
5. **Check Computer Configuration**: To get only the computer configuration data, use the /SCOPE COMPUTER parameter, like gpresult /R /SCOPE COMPUTER.
6. **Check User Configuration**: Similarly, to get only the user configuration data, use the /SCOPE USER parameter, like gpresult /R /SCOPE USER.

7. **Verbose Output**: For a verbose output, which includes more detailed information, use the /V switch, like gpresult /V.
8. **Super Verbose Output**: For even more detailed information, use the /Z switch for a super verbose output. This is particularly useful when you need detailed information on every setting within each applied GPO, like gpresult /Z.
9. **Specify a Destination File**: You can direct the output of gpresult to a text file for easier reading and analysis by using >, like gpresult /R > gpresult.txt.
10. **Troubleshoot Remote Computer**: To troubleshoot GPO issues on a remote computer, use the /S switch followed by the computer name, like gpresult /R /S [computername].

Remember to replace placeholders like [username] and [computername] with actual user names and computer names. The gpresult tool is powerful for diagnosing and troubleshooting Group Policy issues, providing insights into which policies are applied and potentially highlighting any conflicts or errors in GPO application.

Using the Group Policy Results Wizard is an effective way to troubleshoot GPOs

(Group Policy Objects) in a Windows environment. Here are the steps to follow when using this tool:

1. **Open Group Policy Management Console (GPMC)**: You can access GPMC by searching for it in the start menu or by running gpmc.msc via the Run dialog or Command Prompt.
2. **Find the Correct Domain**: In GPMC, navigate to the domain where the target computer or user resides. Ensure you are working in the right domain context.

3. **Start the Group Policy Results Wizard**: Right-click on the "Group Policy Results" node and select "Group Policy Results Wizard" from the context menu.
4. **Select the Target Computer**: The wizard will prompt you to choose a specific computer to analyze. You can browse for the computer or type its name directly. Ensure the computer is online and accessible.
5. **Select the User**: Next, choose the user account for which you want to see the Group Policy results. You can select the current user logged onto the computer or specify another user account.
6. **Review and Run the Report**: Review your selections and run the report. The wizard will connect to the specified computer and gather the Group Policy results for the chosen user.
7. **Analyze the Report**: Once the report is generated, it will appear under the "Group Policy Results" node. This report provides detailed information about:
    - GPOs that were applied or denied and why (such as due to security filtering or WMI filtering).
    - Settings within each GPO that were applied.
    - Any errors or issues encountered during Group Policy processing.
8. **Check for Errors and Warnings**: Pay special attention to any errors or warnings in the report. These often give clues about problems like network connectivity issues, permission problems, or misconfigurations.
9. **Compare Against Expected Results**: Compare the results against what you expected to see in terms of GPO application. This comparison can help identify GPOs that are not applying as intended.
10. **Save or Export the Report**: You can save or export the report for further analysis or for keeping records. The report can be saved in various formats like HTML for easy sharing and viewing.

By following these steps, the Group Policy Results Wizard can provide valuable insights into the Group Policy processing and help in diagnosing and resolving issues with GPO application in your Windows environment.

Using Security Filtering to troubleshoot Group Policy Objects (GPOs)

can help determine whether a GPO is being applied correctly to the intended targets. Here are the steps to use Security Filtering effectively:

1. **Open Group Policy Management Console (GPMC)**: Search for "Group Policy Management" in the start menu or run gpmc.msc from the Run dialog or Command Prompt.
2. **Locate the GPO**: In the GPMC, navigate to the specific GPO you want to troubleshoot. This GPO should be linked to an Organizational Unit (OU) or domain where your target users or computers reside.
3. **Review Current Security Filtering Settings**: Select the GPO and go to the "Scope" tab. Under "Security Filtering", you will see a list of users, groups, or computers that the GPO is currently applied to.
4. **Check for Relevant Groups or Users**: Ensure that the groups or users who need to receive the GPO settings are listed in the Security Filtering section. If they are not listed, they will not receive the GPO settings.
5. **Modify Security Filtering**: To add a group, user, or computer, click on the "Add" button under Security Filtering and enter the name of the group, user, or computer you want to add. To remove, select the entity and click "Remove".
6. **Ensure Proper Permissions**: The objects in Security Filtering must have the "Read" and "Apply Group Policy" permissions for the GPO. This is usually granted by default when you add an object to Security Filtering.
7. **Refresh Group Policy on Target Machines**: Use the gpupdate /force command on the client machines to immediately refresh Group Policy. This helps in quickly verifying if the changes in Security Filtering have taken effect.
8. **Use the Group Policy Results Wizard**: After updating Security Filtering, run the Group Policy Results Wizard in the GPMC against the target user/computer to verify if the GPO is now being applied.
9. **Review Event Logs**: Check the Event Viewer on the client machine for any Group Policy-related errors or warnings, especially if the GPO is still not being applied.
10. **Document Changes**: Keep a record of any changes you make to Security Filtering for future reference and audit purposes.

Remember, Security Filtering is a powerful tool for controlling the scope of GPOs, but it must be used carefully to avoid unintended consequences. Be sure that any changes you make align with your organization's policy and security requirements.

Group Policy Inheritance is a key concept in understanding how Group Policy Objects (GPOs) are applied in a Windows environment.

Troubleshooting GPO issues often involves examining how inheritance is affecting the application of policies. Here are steps to use Group Policy Inheritance effectively for troubleshooting:

1. **Access Group Policy Management Console (GPMC)**: Open GPMC by searching for it in the start menu or by running gpmc.msc through the Run dialog or Command Prompt.
2. **Identify the Target OU**: In GPMC, navigate to the Organizational Unit (OU) where the target users or computers reside. This is where you will examine the inheritance of GPOs.
3. **Review Applied GPOs**: Look at the "Group Policy Inheritance" tab for the OU. This tab shows all GPOs that are applied to this OU, including those inherited from parent OUs or the domain level.
4. **Examine GPO Order**: The order in which GPOs are listed here is important – GPOs at the top of the list have the highest priority, and their settings can override those in GPOs lower down the list.
5. **Check for Block Inheritance**: An OU can be configured to block inheritance, which prevents GPOs linked at higher levels from being automatically applied to the OU. Verify if "Block Inheritance" is enabled for the OU.
6. **Look for Enforced GPOs**: Even if inheritance is blocked, GPOs that are set as "Enforced" at a higher level will still apply. Check for any GPOs marked as "Enforced" in the inheritance chain.
7. **Use the Group Policy Modeling Wizard**: In GPMC, use the Group Policy Modeling Wizard to simulate the effect of inheritance for specific users or computers. This tool can help predict the resultant policy settings.
8. **Analyze Group Policy Results**: Utilize the Group Policy Results tool on a target computer/user to see the actual GPOs applied and in what order. This can help identify any unexpected results due to inheritance.
9. **Troubleshoot Conflicting Settings**: If conflicting settings are detected, determine which GPO has the setting that is prevailing. Adjust the policy settings or the order of GPO application as necessary.
10. **Refresh Group Policy**: After making changes, use gpupdate /force on a client computer to refresh Group Policy immediately and verify if the issue is resolved.
11. **Document Your Findings**: Keep a record of your troubleshooting steps and findings. This can be helpful for future reference or for other administrators.

Understanding and managing Group Policy Inheritance is crucial, especially in complex environments with multiple OUs and GPOs. Properly analyzing how GPOs are inherited and applied can resolve many common issues related to Group Policy application.

Documenting Active Directory (AD) Group Policy Objects (GPOs)

is crucial for effective management, auditing, and troubleshooting. Here are some practical methods for documenting AD GPOs:

1. **Automated Reports Using Group Policy Management Console (GPMC)**:
    - Generate detailed reports for each GPO using the GPMC. These reports can be exported to HTML or XML formats and include all settings within each GPO.
    - Regularly update these reports after any significant change in GPO settings.
2. **Spreadsheet Documentation**:

- Create spreadsheets to document key GPO information like GPO name, description, link location (OU or domain level), security filtering, WMI filters, and main settings.
- Update the spreadsheet whenever a GPO is created, modified, or deleted.

3. **Change Management Logs**:
   - Maintain a log of all changes made to GPOs, including the date of the change, description of what was changed, and the name of the person who made the change.
   - This log can be part of a larger change management database or a simple spreadsheet.
4. **Version Control**:
   - Implement a version control system for GPOs. Whenever a GPO is modified, save a new version of the GPO report.
   - Keep track of the version history in your documentation.
5. **Network Diagrams**:
   - Include GPO information in your network diagrams. Show which GPOs are applied to which OUs or systems.
   - Use diagramming tools like Microsoft Visio to visually represent GPO linkage and inheritance.
6. **Policy Setting Descriptions**:
   - For each GPO, document why each setting was configured a certain way, linking back to business requirements or security policies.
   - This helps in understanding the rationale behind specific configurations.
7. **Backup Documentation**:
   - Document the process and schedule for backing up GPOs.
   - Include information about where backups are stored and how to restore them in case of an emergency.
8. **GPO Testing and Rollout Notes**:
   - Document the process for testing new or modified GPOs in a test environment before deploying them in production.
   - Include details about the test cases, results, and any issues encountered during testing.
9. **Compliance and Audit Reports**:
   - If GPOs are part of compliance requirements (like HIPAA, GDPR, etc.), document how they meet these requirements.
   - Include details from any external or internal audits that involve GPO settings.
10. **User and Administrator Guides**:
    - Create guides for users and administrators explaining the impact of key GPOs, especially those affecting user experience or administrative procedures.
    - Update these guides as policies change.
11. **Access Control and Delegation Records**:

- Document who has edit or read-only access to various GPOs.
- Keep a log of any changes in GPO access control.

By using these methods, you can maintain comprehensive and up-to-date documentation of your AD GPOs, which is essential for effective governance, operational efficiency, and compliance.

Group Policy Examples: Most Useful GPOs for Security

Last Updated: September 10, 2023 by Robert Allen

https://activedirectorypro.com/group-policy-examples-most-useful-gpos-for-security/

This is a list of common Active Directory Group Policies (GPOs) that should be implemented in an Active Directory environment for security and administrative convenience. Please note that not all these settings may be right for your environment so consider each carefully. As with any GPO settings, test on a small group of users and computers before rolling out.

1. Enable Audit Logs

Enabling audit logs helps to monitor activity on your network and is a great security tool for identifying threats in your infrastructure.

At a minimum, you should enable Audit System Events. This policy is in Computer Configuration -> Windows Settings –> Security Settings –> Audit Policy.

Change “Audit System Events” to Success, Failure.

See the article Windows Server Audit Policy for auditing best practices.

2. Screen Lockout Time

Enable a lock-out time from inactivity on your domain computers to protect data and privacy. A generally accepted time is 10 – 15 minutes but can be shorter if need be. Teaching your users to lock their computers when they are walking away from their desks is great. But a backup plan is always ideal.

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Modify the time for Interactive Logon: Machine inactivity limit.

See the article GPO lock screen for more details.

3. Password Policy

Enforcing a strong password policy is critical for the security of your domain.

These settings are in Computer Configuration –> Windows Settings –> Security Settings –> Account Policies –> Password Policy.

See the article Active Directory password policy for more details.

4. Account Lockout Policy

Enforcing an account lockout policy will help keep your domain computers secure. A malicious actor could attempt to guess passwords for a domain account.

These settings are in Computer Configuration –> Windows Settings –> Security Settings –> Account Policies –> Account Lockout Policy.

See the article Active Directory account lockout policy for more details.

5. Removable Media

Allowing your users to plug in USB drives, external hard drives, or insert CDs, DVDs, should be turned off. You open the door up to your network being infected with viruses or malware.

These settings are in User Configuration –> Policies –> Administrative Templates –> System –> Removable Storage Access

You can enable Deny read and execute on specific devices or Enable All Removable Storage classes: Deny all access" to block all devices.

6. Restrict access to the command prompt and PowerShell

Limit access to the command prompt and PowerShell to prevent commands from being run by regular user accounts. If a system is compromised, the command prompt or PowerShell could be used to elevate a user account. Also, PowerShell can be used to run malicious scripts and is often used to spread ransomware.

To prevent access to the command prompt, enable the setting "Prevent access to the command prompt".

The setting is in User Configuration –> Administrative Templates –> System.

To disable PowerShell, see the article disable PowerShell GPO.

7. Limit access to Control Panel options

You should limit access to what users can change in Control Panel. Users can change a lot of system settings in the Control Panel such as network settings, adding and removing software, and adding and removing users. All of these activities could open the door to a security breach.

To lock down access to the control panel, you want to enable "Prohibit access to Control Panel and PC Settings".

This setting is located at User Configuration –> Administrative Templates –> Control Panel

8. Limit who can install software

All software should be tested and approved before being installed on a network. Also, regular user accounts should not be allowed to install software. This is for both security and to alleviate issues the software may cause.

This setting is in Computer Configuration –> Administrative Templates –> Windows Components –> Windows Installer.

Click on "Prohibit User Installs" and enable the policy.

9. Guest Account Settings

Guest accounts grant access to a computer without using a password. This is a security concern as well as a data access concern. It's best to disable guest access.

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies -> Security Options

Click on "Accounts: Guest Account Status" and select disabled.

10. Prevent Storing LAN Manager Hash

LAN Manager stores account passwords in hashes in the local SAM database. The hash is weak and very susceptible to hacking. This should be turned off.

The setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Set "Network Security: Do not store LAN Manager hash value on next password change" policy to Enabled.

11. Limit Local Account use of a blank password to console only

Blank passwords are a high-security threat. In the case that an admin inadvertently creates a local account with no password before it is added to the domain, you can block the ability for that account to be used via RDP, Telnet, and FTP.

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Set "Accounts: Limit local account use of blank password to console logon only" to Enabled.

12. Turn off forced restarts

If you are using Windows Update, disable automatic restarts when users are logged on. This will prevent a lot of angry emails and phone calls.

This setting is in Computer Configuration –> Administrative Templates –> Windows Components –> Windows Updates.

Enable the policy "No auto-restart with logged on users for scheduled automatic updates installations".

13. Monitor Changes to GPO Settings

Tracking changes to your Group Policy Object settings is very helpful when you have multiple admins making changes.

This setting is in Computer Configuration –> Policies –> Windows Settings –> Security Settings –> Advanced Audit Policy Configuration –> Audit Policies/DS Access.

Select Audit Directory Service Changes and click Success.

14. Block Microsoft Store

Users can get carried away with launching apps from Microsoft Store. This creates an admin nightmare.

To block Microsoft Store, Enable the setting “Turn off the store application”.

This setting is in Computer Configuration –> Administrative Templates -> Windows Components –> Store

There are some apps that still require updating via Microsoft Store, you can allow this by going to Computer Configuration –> Administrative Templates –> Windows Components –> Store.

Select the policy “Turn off automatic download and install of updates” and select disable.

15. Disable Anonymous SID/Name Translation

If this option is enabled, it is possible using the SID to get the name of the built-in Administrator account even if the admin account has been changed to a different name.

The setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Change the policy “Network access: Allow anonymous SID/Name translation” to Disabled.

16. Limit access to the Registry

Altering the registry settings is always a major concern for admins. You can lock down the registry so that users can’t alter it.

This setting is in User Configuration –> Administrative Templates –> System.

Select the policy “Prevent access to registry editing tools” and set it to Enabled.

Then under Disable regedit from running silently, change to Yes.

17. Remove Anonymous Users from Everyone Permissions

This should be disabled by default. I would double-check. If this is enabled, anonymous users can access any resources that everyone permissions have access to.

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options

“Network access: Let everyone permissions apply to anonymous users” should be set to Disabled.

18. Turn on auditing for NTLM to make sure you are not using it.

NTLM is a legacy authentication protocol and has several vulnerabilities, it was replaced with Kerberos in Windows 2000. Before you disable it, make sure you don’t have any legacy clients still using these authentication methods.

Audit NTLM Usage

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Select policy “Network Security: Restrict NTLM: Audit NTLM authentication in this domain” and enable all.

You can view the Event Viewer under Applications and Services Log – Microsoft – Windows – NTLM to see if NTLM is being used. Look for NTLM in the Authentication Package value. The Package name will show you what version of NTLM is being used.

After making sure your domain is not using NTLM, you can disable it.

Disable NTLM (Make sure you audit your network first)

This setting is in Computer Configuration –> Windows Settings –> Security Settings –> Local Policies –> Security Options.

Select policy “Network Security: Restrict NTLM: NTLM authentication in this domain” and select Deny All.

19. Disable LLMNR

Link local Multicast Name Resolution (LLMNR) is a protocol used to resolve IP Addresses to host names. Basically, it performs domain name lookups without a DNS server. It works by sending a broadcast out on the network looking for an address and any devices on the network can respond. This can easily be used by an attacker to respond to these broadcasts and connect to machines. In a business network, your devices should be using a DNS server you control or approve.

You can disable LLMNR with this policy setting.

Computer Configuration -> Administrative Templates -> Network -> DNS ClientEnable Turn Off Multicast Name Resolution policy by changing its value to Enabled

20. Control the Local Administrators Group

If you do not limit access to the local administrator's group then how do you know which accounts are full administrator rights? Over time staff will create and add existing accounts into the local administrator's group on workstations and laptops. This will give the account full rights to the computer allowing them to install software, and drivers, make system changes, and so on. This is bad security practice and no user should be doing their day to day work with full administrator rights.

You can use group policy to control which users are members of this group and prevent other staff from making changes.

Refer to the remove local admin rights guide for step-by-step instructions.

21. Windows Firewall

I recommend you centrally manage the Windows firewall using group policy. This is similar to the local administrator rights issue, if you are not centrally managing it the rules can get out of control. If a user gets a firewall prompt to allow or deny something that could easily click allow all the time. Any requests to unblock something should come through the IT/Security team.

See the article Windows firewall best practices for more details.

22. Enable User Account Control (UAC)

With UAC, applications run in the security context of a regular user (non-administrator account) and it prompts for permissions when the application needs administrator-level access.

This is another layer of security to help protect users, computers, and your network. This is another setting that users or other staff can disable. Use group policy to centrally force UAC to be enabled and prevent it from being disabled.

The UAC policies are located in the following:

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.

23. Applocker or Software Restriction Policies

Applocker is a feature that allows you to control which applications and files can run. This can help prevent unapproved software and files from running. For example, if a user downloads software from the internet and it is not approved in the Applocker policy the software will be blocked.

This can also help prevent ransomware and other malicious viruses from installing and spreading on your network. Applocker is only available on Windows enterprise addition. If you are running Windows pro then look into software restriction policies.

The software restriction policies are located in the following.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Software restiriction policies

I hope you enjoyed this article. What GPOs do you use to improve security?

Tools to help with group policy design

Posted by Dishan M. Francis | May 28, 2015 | Active Directory, MICROSOFT, Windows 2012, Windows Server 2008 | 0 |

Last Updated on May 28, 2015 by Dishan M. Francis

Design a group policies for organization some time getting more complex. It can make chaos as some time it very hard to revert back the changes pushed from group policies to workstations. Especially things which involves with registry value changes. So proper design is very important.

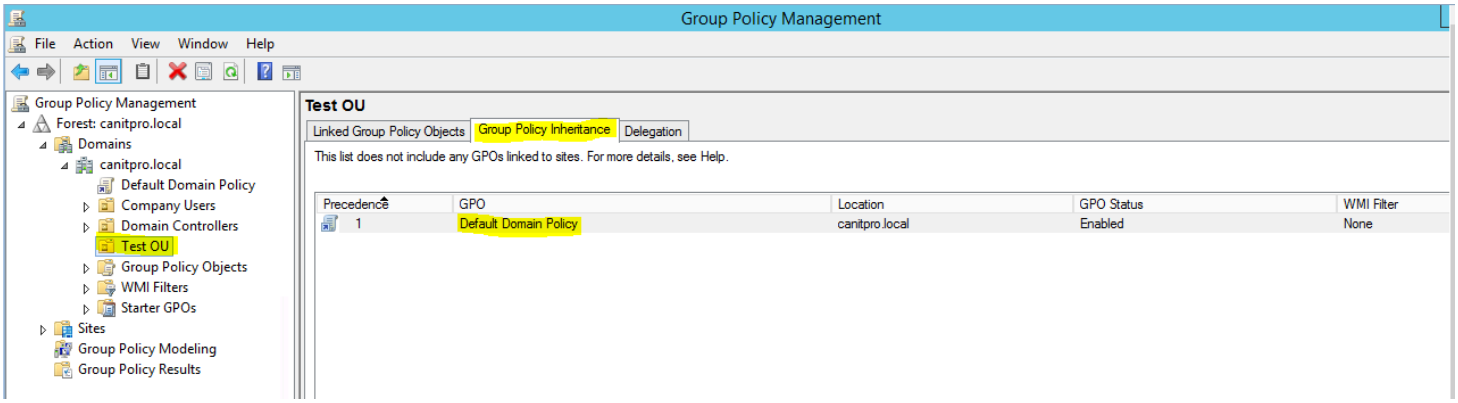
There are some tools/features comes GPO management which can help with design, test or troubleshooting group policies. Please note none of these recommended to use as permanent solutions to fix group policy design issues.

Block Inheritance

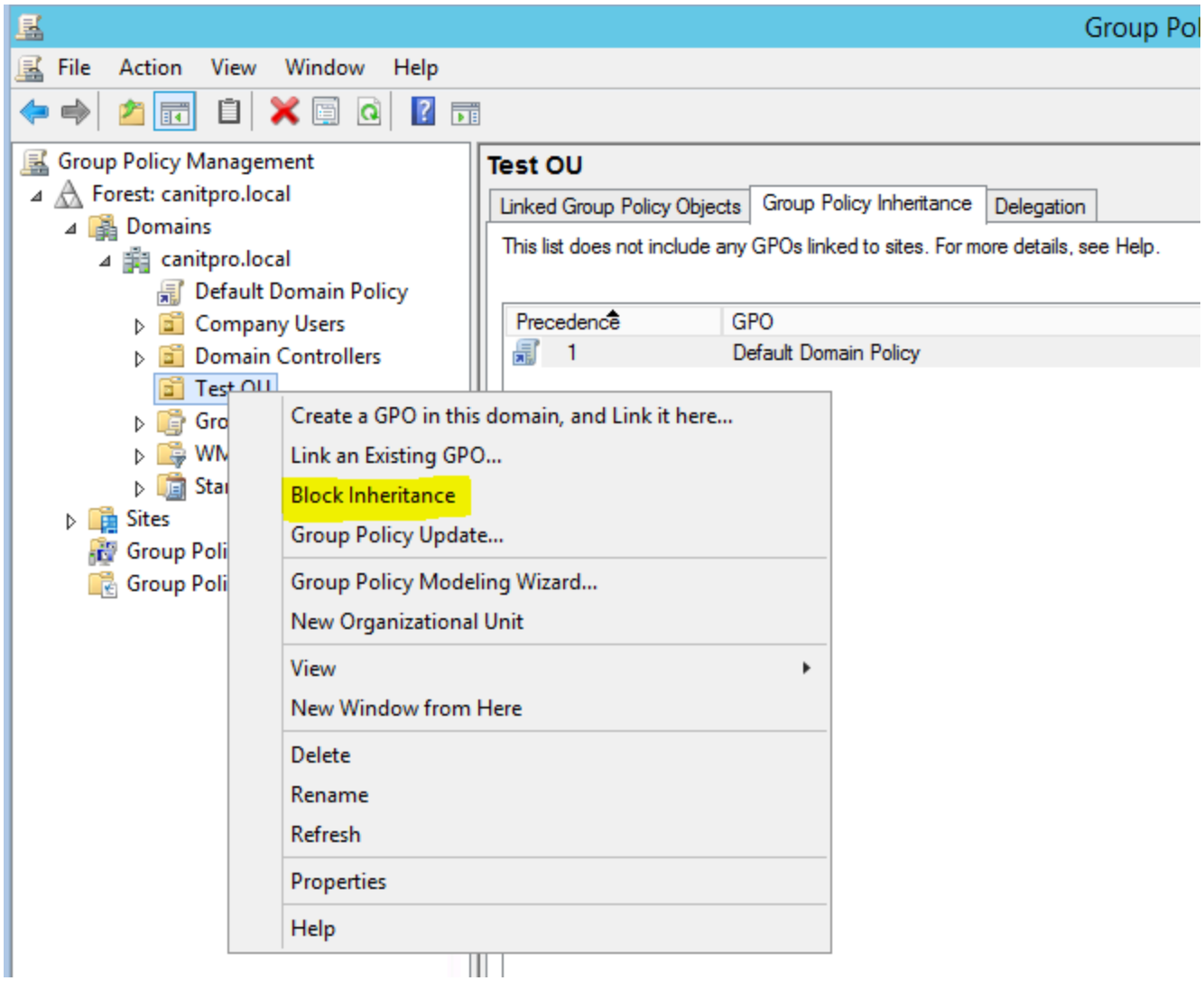
Any GPO setup on the higher level in GPO structure automatically applies to the lower level in the model. For example the "**Default Domain Policy**" by default in the highest level in

structure. So any changes done on that (which is not recommended) also applies to lower level in hierarchy.

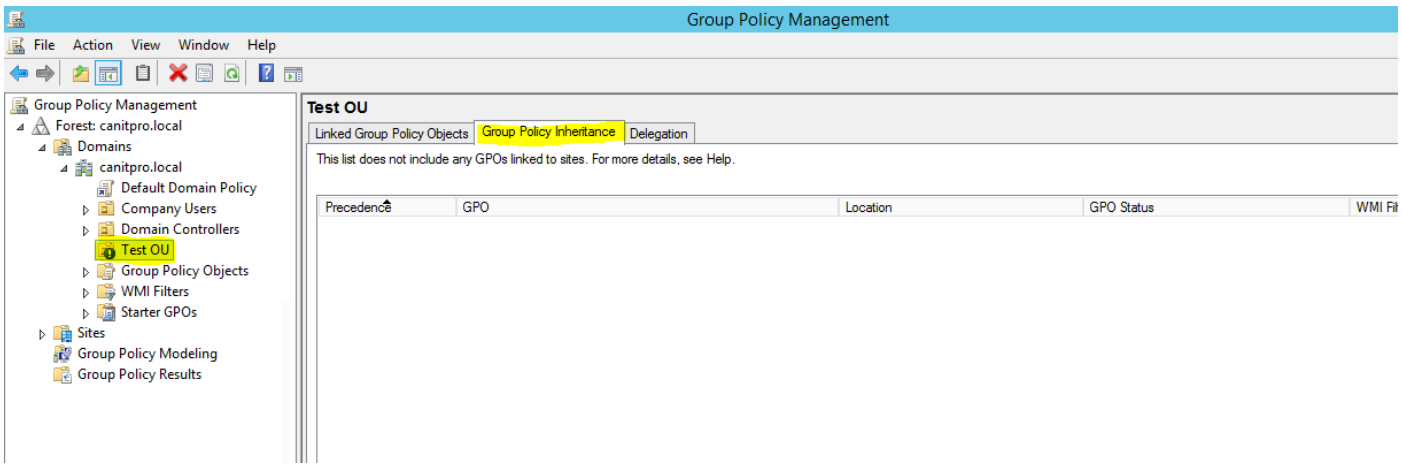
In following screenshot, as you can see the default domain policy is automatically inherited to "**Test OU**" I have created.



We can disable this inheritance. To do that, right click on the OU which we need to block the inheritance and click "**Block Inheritance**".



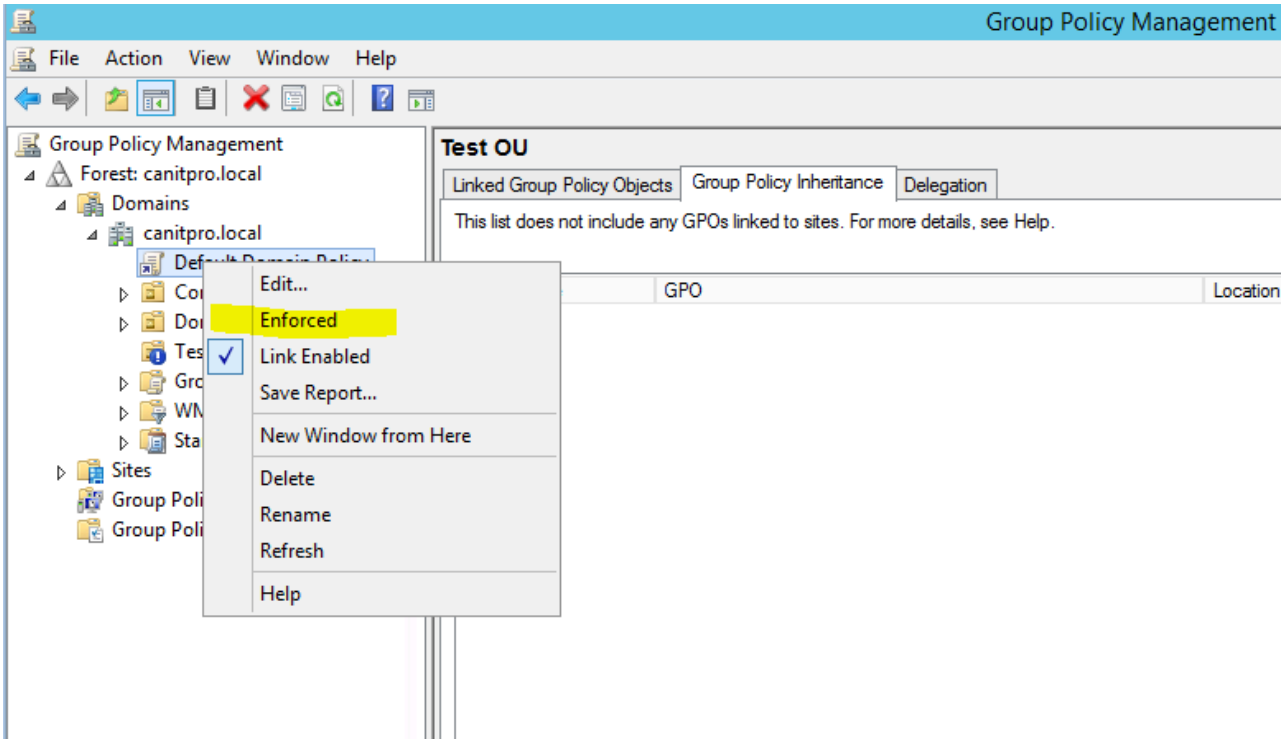
Once it's done, we no longer can see the default domain policy which was inherited.



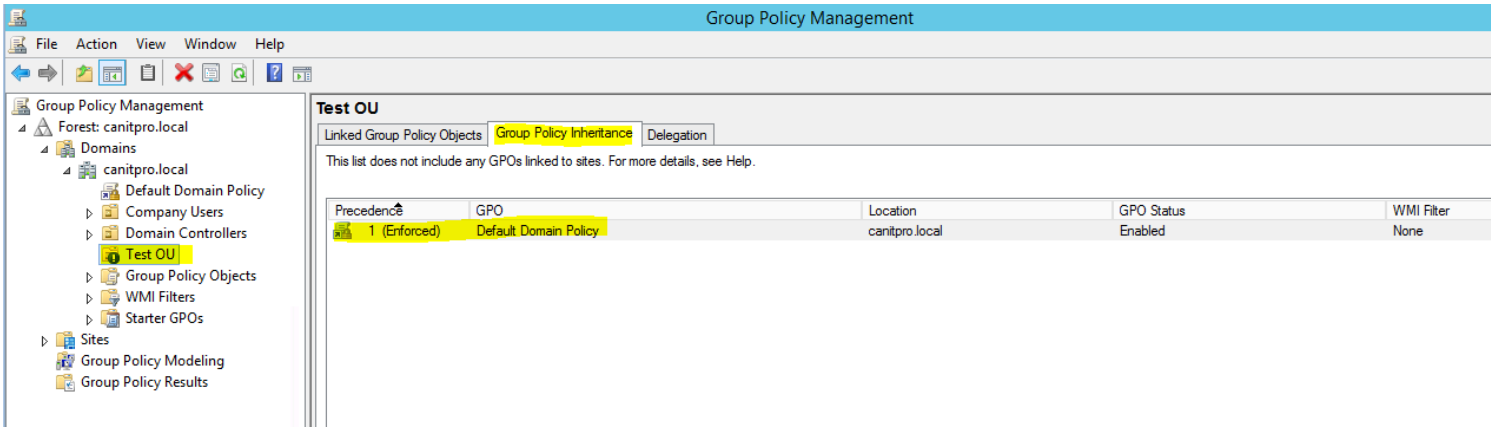
Enforced Policies

Using enforced policy option we can enforce policies to apply on lower level in hierarchy. For example let's assume we have two polices called Policy A and Policy B in height level in hierarchy. In lower level in hierarchy some OU are blocked policy inheritance so these 2 policies by default will not apply to those two. But we still need to push Policy A for everyone in organization no matter what. So by enforcing the policy we can even push it to the OUs even its use block inheritance.

To enforce a policy, right click on the policy you needs to enforce and click on "Enforced".



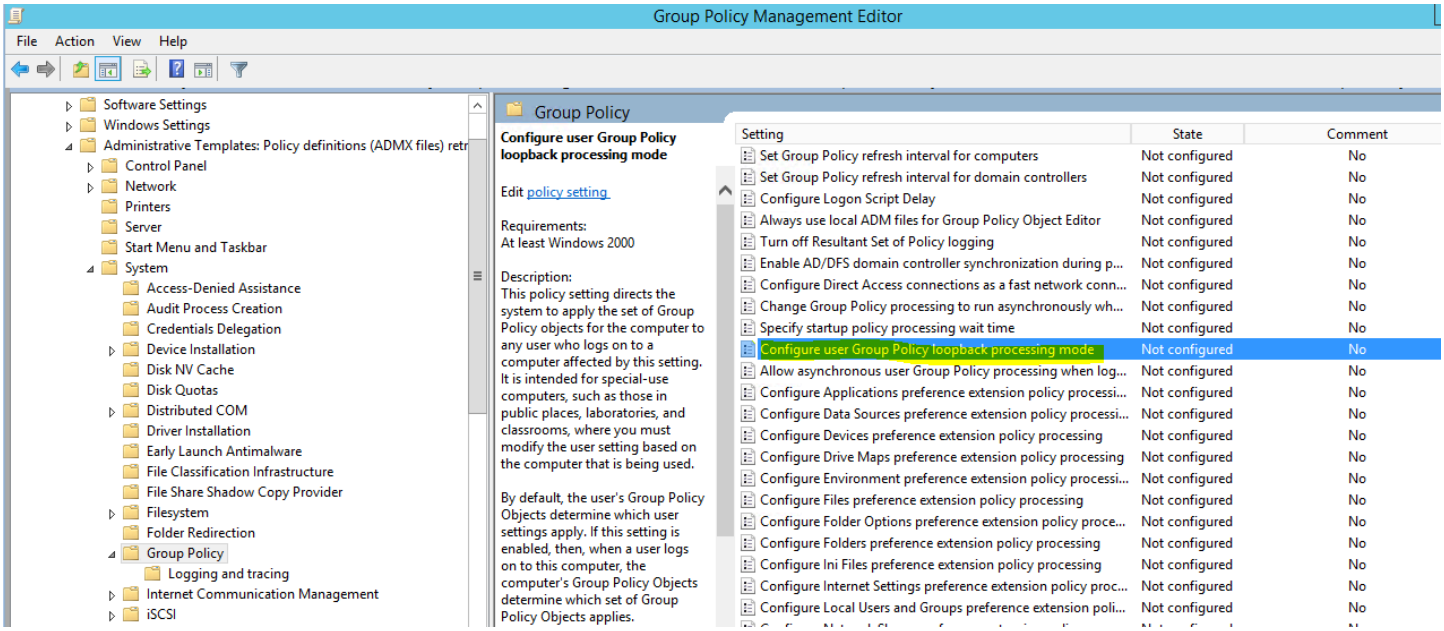
Then we can see in Test OU, it is inherited even its use block inheritance option.



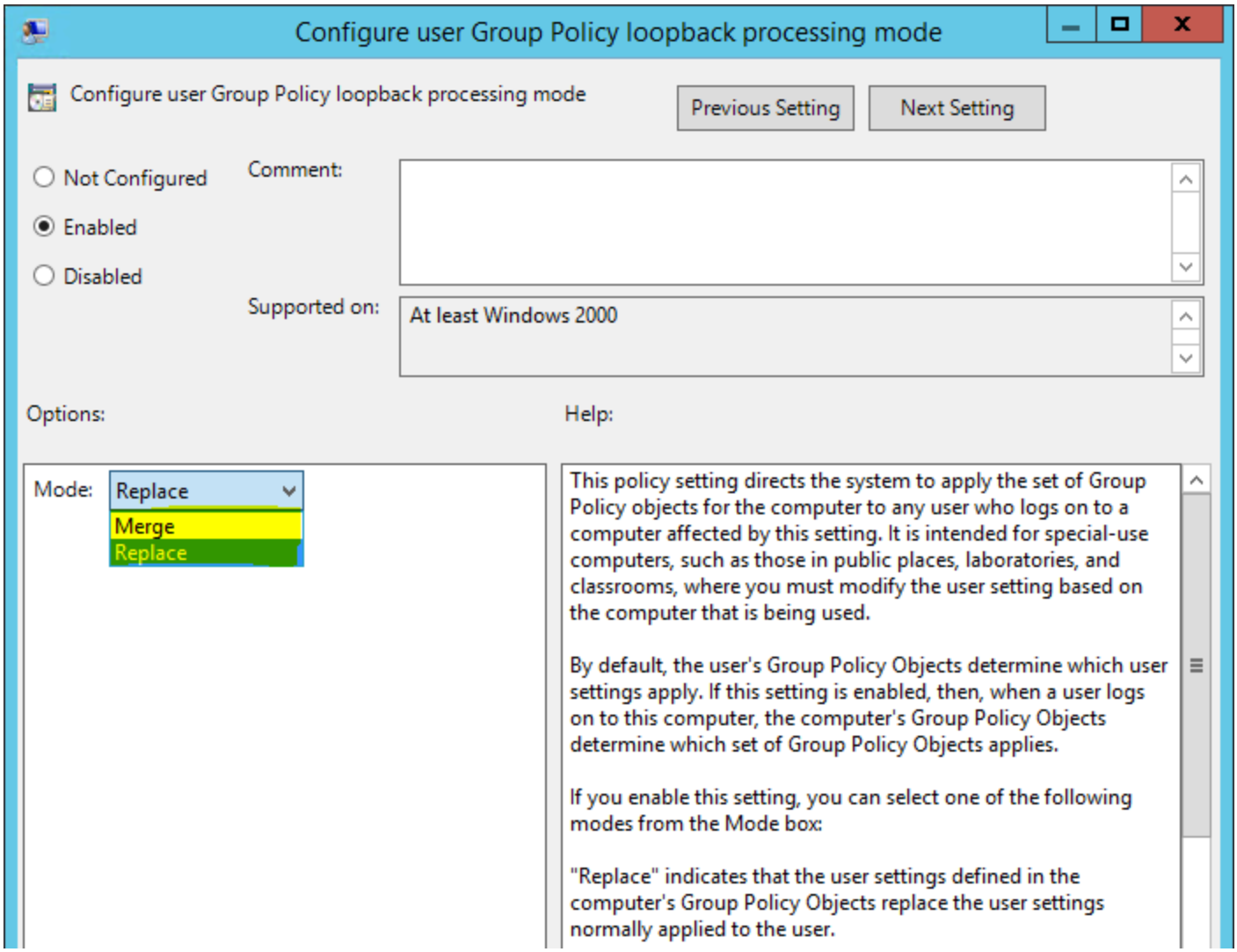
Loopback Processing

As we know we can apply group policies based on the user object or the computer object n active directory. But some special occasions we need to only consider the policies based on computer object. For ex- in a library or public lab, many users may uses the same computer. In that case the computer should stay same for every users. It should not change based on the user policies. It only should use the computer policies which is applied to it.

In group policy management, start to edit the policy you like to configure with loopback processing. Under Computer Configuration\Policies\Administrative Templates\System\Group Policies\ double click on the option “Configure user Group Policy loopback processing mode”.



There are 2 modes we can use with it.



Replace – This will not consider about user polices at all. It will only apply the computer GPO.
Merge – in this mode it will consider both user and computer polices. But if there is any conflict it always uses the computer policies.

Group Policies in a traditional on-premises Active Directory (AD) environment are a well-established method for managing and configuring operating systems, applications, and user settings. However, in Azure, especially with Azure Active Directory (Azure AD), the approach to policy management differs somewhat due to the nature of cloud services and the lack of traditional domain-joined scenarios.

Here's how Group Policies work in Azure:

1. **Azure Active Directory (Azure AD)**: Azure AD is a cloud-based identity and access management service. It doesn't natively support Group Policy in the same way as on-premises Active Directory. Azure AD focuses more on identity management, access control, and security compliance, rather than detailed OS or application-level settings.
2. **Azure AD Domain Services (Azure AD DS)**: For scenarios requiring traditional AD capabilities, including Group Policy, Azure offers Azure AD Domain Services. Azure AD DS provides managed domain services such as domain join, LDAP, Kerberos/NTLM authentication, and Group Policy support. It enables you to leverage Group Policy in Azure much like you would in an on-premises AD environment.
3. **Group Policy in Azure AD DS**: In Azure AD DS, you can manage Group Policy Objects (GPOs) through the Group Policy Management Console (GPMC), similar to managing GPOs in an on-premises domain. You can configure policies for users and computers that are part of the Azure AD DS domain.
4. **Intune for Policy Management**: Microsoft Intune, part of Microsoft's Enterprise Mobility + Security (EMS) suite, is often used in conjunction with Azure AD for device and application management. Intune provides policy management features that can be considered a modern, cloud-based alternative to certain aspects of Group Policy. While not a direct replacement, Intune offers extensive policy management capabilities for mobile devices and PCs, including settings specific to Windows 10.
5. **Conditional Access Policies**: Azure AD includes conditional access policies that provide a level of control over how resources are accessed. While not the same as Group Policy, conditional access policies are crucial for securing access in a cloud-centric environment.
6. **Hybrid Environments**: In hybrid environments where on-premises AD is integrated with Azure AD (using Azure AD Connect), Group Policies applied on-premises can still affect domain-joined machines, while Azure-based services leverage Azure AD and Intune for policy management.
7. **Migration and Coexistence**: Organizations migrating to Azure often need to consider how to transition their Group Policy strategy. This might involve using Azure AD DS for traditional Group Policy support or adopting Intune for a more modern management approach.

In summary, while Azure doesn’t support Group Policies in the same way as on-premises Active Directory, Azure AD Domain Services can provide similar functionality for certain scenarios. For modern device management and configuration in the cloud, Microsoft Intune is the preferred tool, offering extensive policy management capabilities that align with cloud-based infrastructure and services.

Security policy settings

- 02/16/2023

In this article

Applies to

- Windows 10
- Windows 11

This reference topic describes the common scenarios, architecture, and processes for security settings.

Security policy settings are rules that administrators configure on a computer or multiple devices for protecting resources on a device or network. The Security Settings extension of the Local Group Policy Editor snap-in allows you to define security configurations as part of a Group Policy Object (GPO). The GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain. Security settings policies are used as part of your overall security implementation to help secure domain controllers, servers, clients, and other resources in your organization.

Security settings can control:

- User authentication to a network or device.
- The resources that users are permitted to access.
- Whether to record a user's or group's actions in the event log.

- Membership in a group.

To manage security configurations for multiple devices, you can use one of the following options:

- Edit specific security settings in a GPO.
- Use the Security Templates snap-in to create a security template that contains the security policies you want to apply, and then import the security template into a Group Policy Object. A security template is a file that represents a security configuration, and it can be imported to a GPO, applied to a local device, or used to analyze security.

For more info about managing security configurations, see Administer security policy settings.

The Security Settings extension of the Local Group Policy Editor includes the following types of security policies:

- **Account Policies.** These policies are defined on devices; they affect how user accounts can interact with the computer or domain. Account policies include the following types of policies:
    - **Password Policy.** These policies determine settings for passwords, such as enforcement and lifetimes. Password policies are used for domain accounts.
    - **Account Lockout Policy.** These policies determine the conditions and length of time that an account will be locked out of the system. Account lockout policies are used for domain or local user accounts.
    - **Kerberos Policy.** These policies are used for domain user accounts; they determine Kerberos-related settings, such as ticket lifetimes and enforcement.
- **Local Policies.** These policies apply to a computer and include the following types of policy settings:
    - **Audit Policy.** Specify security settings that control the logging of security events into the Security log on the computer, and specifies what types of security events to log (success, failure, or both).

Note

For devices running Windows 7 and later, we recommend to use the settings under Advanced Audit Policy Configuration rather than the Audit Policy settings under Local Policies.

- **User Rights Assignment.** Specify the users or groups that have sign-in rights or privileges on a device
- **Security Options.** Specify security settings for the computer, such as Administrator and Guest Account names; access to floppy disk drives and CD-ROM drives; installation of drivers; sign-in prompts; and so on.

- **Windows Firewall with Advanced Security.** Specify settings to protect the device on your network by using a stateful firewall that allows you to determine which network traffic is permitted to pass between your device and the network.
- **Network List Manager Policies.** Specify settings that you can use to configure different aspects of how networks are listed and displayed on one device or on many devices.
- **Public Key Policies.** Specify settings to control Encrypting File System, Data Protection, and BitLocker Drive Encryption in addition to certain certificate paths and services settings.
- **Software Restriction Policies.** Specify settings to identify software and to control its ability to run on your local device, organizational unit, domain, or site.
- **Application Control Policies.** Specify settings to control which users or groups can run particular applications in your organization based on unique identities of files.
- **IP Security Policies on Local Computer.** Specify settings to ensure private, secure communications over IP networks by using cryptographic security services. IPsec establishes trust and security from a source IP address to a destination IP address.
- **Advanced Audit Policy Configuration.** Specify settings that control the logging of security events into the security log on the device. The settings under Advanced Audit Policy Configuration provide finer control over which activities to monitor as opposed to the Audit Policy settings under Local Policies.

Windows edition and licensing requirements

The following table lists the Windows editions that support Windows security policy settings and auditing:

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
Yes	Yes	Yes	Yes

Windows security policy settings and auditing license entitlements are granted by the following licenses:

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
Yes	Yes	Yes	Yes	Yes

For more information about Windows licensing, see Windows licensing overview.

Policy-based security settings management

The Security Settings extension to Group Policy provides an integrated policy-based management infrastructure to help you manage and enforce your security policies.

You can define and apply security settings policies to users, groups, and network servers and clients through Group Policy and Active Directory Domain Services (AD DS). A group of servers with the same functionality can be created (for example, a Microsoft Web (IIS) server), and then Group Policy Objects can be used to apply common security settings to the group. If more servers are added to this group later, many of the common security settings are automatically applied, reducing deployment and administrative labor.

Common scenarios for using security settings policies

Security settings policies are used to manage the following aspects of security: accounts policy, local policy, user rights assignment, registry values, file and registry Access Control Lists (ACLs), service startup modes, and more.

As part of your security strategy, you can create GPOs with security settings policies configured specifically for the various roles in your organization, such as domain controllers, file servers, member servers, clients, and so on.

You can create an organizational unit (OU) structure that groups devices according to their roles. Using OUs is the best method for separating specific security requirements for the different roles in your network. This approach also allows you to apply customized security templates to each class of server or computer. After creating the security templates, you create a new GPO for each of the OUs, and then import the security template (.inf file) into the new GPO.

Importing a security template to a GPO ensures that any accounts to which the GPO is applied automatically receive the template's security settings when the Group Policy settings are refreshed. On a workstation or server, the security settings are refreshed at regular intervals

(with a random offset of at most 30 minutes), and, on a domain controller, this process occurs every few minutes if changes have occurred in any of the GPO settings that apply. The settings are also refreshed every 16 hours, whether or not any changes have occurred.

Note

These refresh settings vary between versions of the operating system and can be configured.

By using Group Policy–based security configurations in conjunction with the delegation of administration, you can ensure that specific security settings, rights, and behavior are applied to all servers and computers within an OU. This approach makes it simple to update many servers with any other changes required in the future.

Dependencies on other operating system technologies

For devices that are members of a Windows Server 2008 or later domain, security settings policies depend on the following technologies:

- **Active Directory Domain Services (AD DS)**

The Windows-based directory service, AD DS, stores information about objects on a network and makes this information available to administrators and users. By using AD DS, you can view and manage network objects on the network from a single location, and users can access permitted network resources by using a single sign in.

- **Group Policy**

The infrastructure within AD DS that enables directory-based configuration management of user and computer settings on devices running Windows Server. By using Group Policy, you can define configurations for groups of users and computers, including policy settings, registry-based policies, software installation, scripts, folder redirection, Remote Installation Services, Internet Explorer maintenance, and security.

- **Domain Name System (DNS)**

A hierarchical naming system used for locating domain names on the Internet and on private TCP/IP networks. DNS provides a service for mapping DNS domain names to IP addresses, and IP addresses to domain names. This service allows users, computers, and applications to query DNS to specify remote systems by fully qualified domain names rather than by IP addresses.

- **Winlogon**

A part of the Windows operating system that provides interactive logon support. Winlogon is designed around an interactive logon model that consists of three components: the Winlogon executable, a credential provider, and any number of network providers.

- **Setup**

Security configuration interacts with the operating system setup process during a clean installation or upgrade from earlier versions of Windows Server.

- **Security Accounts Manager (SAM)**

A Windows service used during the sign-in process. SAM maintains user account information, including groups to which a user belongs.

- **Local Security Authority (LSA)**

A protected subsystem that authenticates and signs in users to the local system. LSA also maintains information about all aspects of local security on a system, collectively known as the Local Security Policy of the system.

- **Windows Management Instrumentation (WMI)**

A feature of the Microsoft Windows operating system, WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI provides access to information about objects in a managed environment. Through WMI and the WMI application programming interface (API), applications can query for and make changes to static information in the Common Information Model (CIM) repository and dynamic information maintained by the various types of providers.

- **Resultant Set of Policy (RSoP)**

An enhanced Group Policy infrastructure that uses WMI in order to make it easier to plan and debug policy settings. RSoP provides public methods that expose what an extension to Group Policy would do in a what-if situation, and what the extension has done in an actual situation. These public methods allow administrators to easily determine the combination of policy settings that apply to, or will apply to, a user or device.

- **Service Control Manager (SCM)**

Used for configuration of service startup modes and security.

- **Registry**

Used for configuration of registry values and security.

- **File system**

Used for configuration of security.

- **File system conversions**

Security is set when an administrator converts a file system from FAT to NTFS.

- **Microsoft Management Console (MMC)**

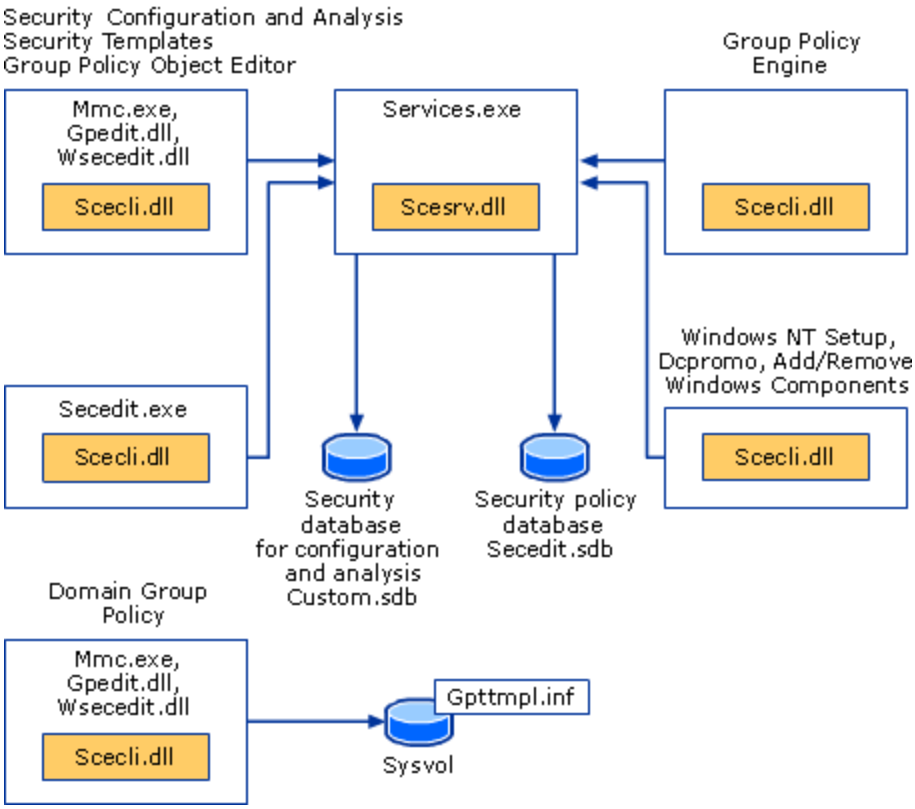
The user interface for the Security Settings tool is an extension of the Local Group Policy Editor MMC snap-in.

Security settings policies and Group Policy

The Security Settings extension of the Local Group Policy Editor is part of the Security Configuration Manager tool set. The following components are associated with Security Settings: a configuration engine; an analysis engine; a template and database interface layer; setup integration logic; and the secedit.exe command-line tool. The security configuration engine is responsible for handling security configuration editor-related security requests for the system on which it runs. The analysis engine analyzes system security for a given configuration and saves the result. The template and database interface layer handles reading and writing requests from and to the template or database (for internal storage). The Security Settings extension of the Local Group Policy Editor handles Group Policy from a domain-based or local device. The security configuration logic integrates with setup and manages system security for a clean installation or upgrade to a more recent Windows operating system. Security information is stored in templates (.inf files) or in the Secedit.sdb database.

The following diagram shows Security Settings and related features.

Security Settings Policies and Related Features



- **Scesrv.dll**

Provides the core security engine functionality.

- **Scecli.dll**

Provides the client-side interfaces to the security configuration engine and provides data to Resultant Set of Policy (RSoP).

- **Wsecedit.dll**

The Security Settings extension of Local Group Policy Editor. scecli.dll is loaded into wsecedit.dll to support the Security Settings user interface.

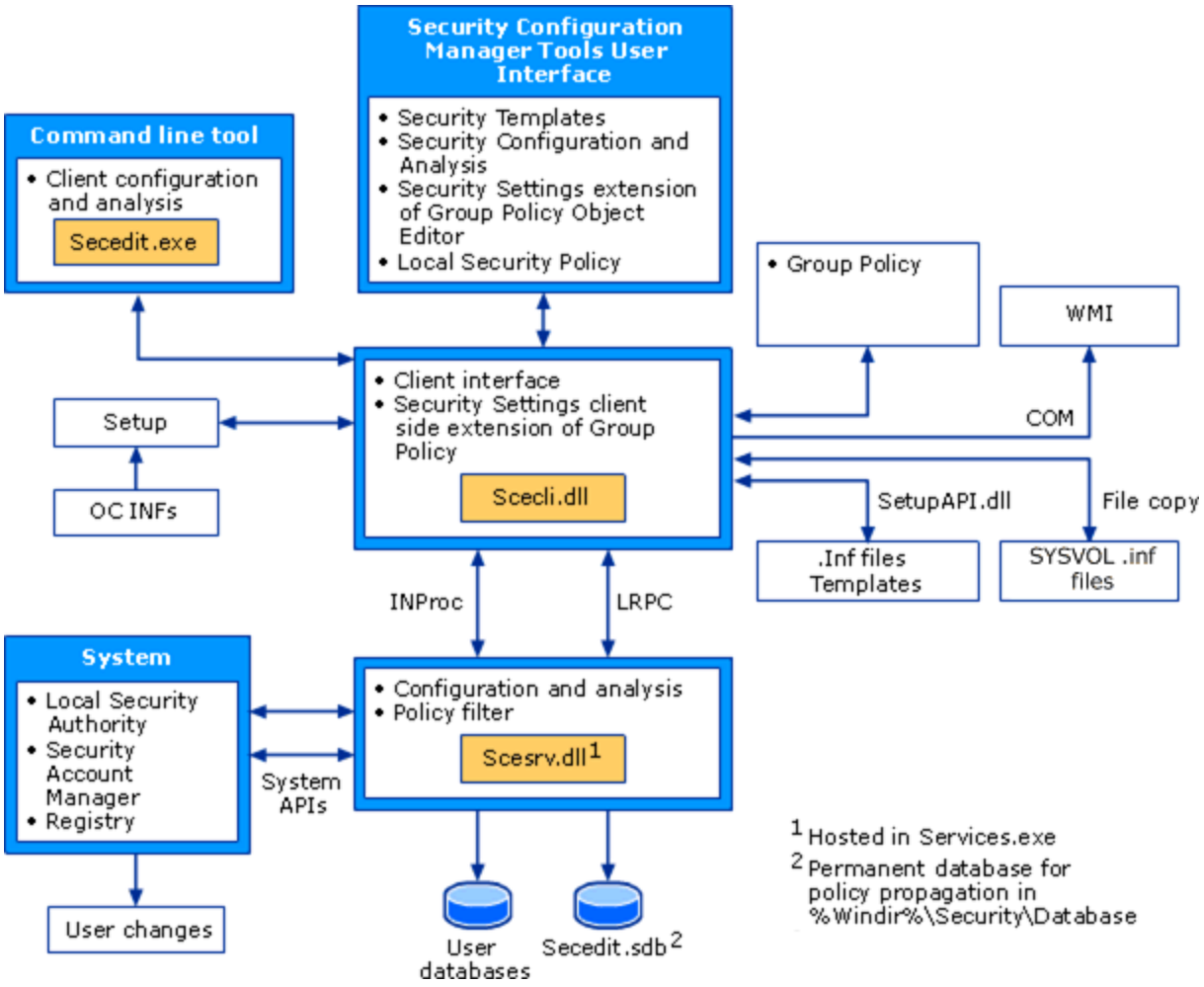
- **Gpedit.dll**

The Local Group Policy Editor MMC snap-in.

Security Settings extension architecture

The Security Settings extension of the Local Group Policy Editor is part of the Security Configuration Manager tools, as shown in the following diagram.

Security Settings Architecture



The security settings configuration and analysis tools include a security configuration engine, which provides local computer (non-domain member) and Group Policy–based configuration and analysis of security settings policies. The security configuration engine also supports the creation of security policy files. The primary features of the security configuration engine are scecli.dll and scesrv.dll.

The following list describes these primary features of the security configuration engine and other Security Settings–related features.

- **scesrv.dll**

This .dll file is hosted in services.exe and runs under local system context. scesrv.dll provides core Security Configuration Manager functionality, such as import, configure, analyze, and policy propagation.

Scesrv.dll performs configuration and analysis of various security-related system parameters by calling corresponding system APIs, including LSA, SAM, and the registry.

Scesrv.dll exposes APIs such as import, export, configure, and analyze. It checks that the request is made over LRPC (Windows XP) and fails the call if it isn't.

Communication between parts of the Security Settings extension occurs by using the following methods:

- Component Object Model (COM) calls
- Local Remote Procedure Call (LRPC)
- Lightweight Directory Access Protocol (LDAP)
- Active Directory Service Interfaces (ADSI)
- Server Message Block (SMB)
- Win32 APIs
- Windows Management Instrumentation (WMI) calls

On domain controllers, scesrv.dll receives notifications of changes made to SAM and the LSA that need to be synchronized across domain controllers. Scesrv.dll incorporates those changes into the Default Domain Controller Policy GPO by using in-process scecli.dll template modification APIs. Scesrv.dll also performs configuration and analysis operations.

- **Scecli.dll**

This Scecli.dll is the client-side interface or wrapper to scesrv.dll. scecli.dll is loaded into Wsecedit.dll to support MMC snap-ins. It's used by Setup to configure default system security and security of files, registry keys, and services installed by the Setup API .inf files.

The command-line version of the security configuration and analysis user interfaces, secedit.exe, uses scecli.dll.

Scecli.dll implements the client-side extension for Group Policy.

Scesrv.dll uses scecli.dll to download applicable Group Policy files from SYSVOL in order to apply Group Policy security settings to the local device.

Scecli.dll logs application of security policy into WMI (RSoP).

Scesrv.dll policy filter uses scecli.dll to update Default Domain Controller Policy GPO when changes are made to SAM and LSA.

- **Wsecedit.dll**

The Security Settings extension of the Group Policy Object Editor snap-in. You use this tool to configure security settings in a Group Policy Object for a site, domain, or organizational unit. You can also use Security Settings to import security templates to a GPO.

- **Secedit.sdb**

This Secedit.sdb is a permanent system database used for policy propagation including a table of persistent settings for rollback purposes.

- **User databases**

A user database is any database other than the system database created by administrators for the purposes of configuration or analysis of security.

- **.Inf Templates**

These templates are text files that contain declarative security settings. They're loaded into a database before configuration or analysis. Group Policy security policies are stored in .inf files on the SYSVOL folder of domain controllers, where they're downloaded (by using file copy) and merged into the system database during policy propagation.

Security settings policy processes and interactions

For a domain-joined device, where Group Policy is administered, security settings are processed in conjunction with Group Policy. Not all settings are configurable.

Group Policy processing

When a computer starts and a user signs in, computer policy and user policy are applied according to the following sequence:

1. The network starts. Remote Procedure Call System Service (RPCSS) and Multiple Universal Naming Convention Provider (MUP) start.
2. An ordered list of Group Policy Objects is obtained for the device. The list might depend on these factors:
    - Whether the device is part of a domain and, therefore, subject to Group Policy through Active Directory.
    - The location of the device in Active Directory.
    - Whether the list of Group Policy Objects has changed. If the list of Group Policy Objects hasn't changed, no processing is done.

3. Computer policy is applied. These settings are the ones under Computer Configuration from the gathered list. This process is a synchronous one by default and occurs in the following order: local, site, domain, organizational unit, child organizational unit, and so on. No user interface appears while computer policies are processed.
4. Startup scripts run. These scripts are hidden and synchronous by default; each script must complete or time out before the next one starts. The default time-out is 600 seconds. You can use several policy settings to modify this behavior.
5. The user presses CTRL+ALT+DEL to sign in.
6. After the user is validated, the user profile loads; it's governed by the policy settings that are in effect.
7. An ordered list of Group Policy Objects is obtained for the user. The list might depend on these factors:
    - Whether the user is part of a domain and, therefore, subject to Group Policy through Active Directory.
    - Whether loopback policy processing is enabled, and if so, the state (Merge or Replace) of the loopback policy setting.
    - The location of the user in Active Directory.
    - Whether the list of Group Policy Objects has changed. If the list of Group Policy Objects hasn't changed, no processing is done.
8. User policy is applied. These settings are the ones under User Configuration from the gathered list. These settings are synchronous by default and in the following order: local, site, domain, organizational unit, child organizational unit, and so on. No user interface appears while user policies are processed.
9. Logon scripts run. Group Policy–based logon scripts are hidden and asynchronous by default. The user object script runs last.
10. The operating system user interface that is prescribed by Group Policy appears.

Group Policy Objects storage

A Group Policy Object (GPO) is a virtual object that is identified by a Globally Unique Identifier (GUID) and stored at the domain level. The policy setting information of a GPO is stored in the following two locations:

- **Group Policy containers in Active Directory.**

The Group Policy container is an Active Directory container that contains GPO properties, such as version information, GPO status, plus a list of other component settings.

- **Group Policy templates in a domain's system volume folder (SYSVOL).**

The Group Policy template is a file system folder that includes policy data specified by .admx files, security settings, script files, and information about applications that are available for installation. The Group Policy template is located in the SYSVOL folder in the <domain>\Policies subfolder.

The **GROUP_POLICY_OBJECT** structure provides information about a GPO in a GPO list, including the version number of the GPO, a pointer to a string that indicates the Active Directory portion of the GPO, and a pointer to a string that specifies the path to the file system portion of the GPO.

Group Policy processing order

Group Policy settings are processed in the following order:

1. **Local Group Policy Object.**

Each device running a Windows operating system beginning with Windows XP has exactly one Group Policy Object that is stored locally.

2. **Site.**

Any Group Policy Objects that have been linked to the site are processed next. Processing is synchronous and in an order that you specify.

3. **Domain.**

Processing of multiple domain-linked Group Policy Objects is synchronous and in an order you specify.

4. **Organizational units.**

Group Policy Objects that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then Group Policy Objects that are linked to its child organizational unit, and so on. Finally, the Group Policy Objects that are linked to the organizational unit that contains the user or device are processed.

At the level of each organizational unit in the Active Directory hierarchy, one, many, or no Group Policy Objects can be linked. If several Group Policy Objects are linked to an organizational unit, their processing is synchronous and in an order that you specify.

This order means that the local Group Policy Object is processed first, and Group Policy Objects that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites the earlier Group Policy Objects.

This order is the default processing order and administrators can specify exceptions to this order. A Group Policy Object that is linked to a site, domain, or organizational unit (not a local Group Policy Object) can be set to **Enforced** with respect to that site, domain, or organizational unit, so that none of its policy settings can be overridden. At any site, domain, or organizational unit, you can mark Group Policy inheritance selectively as **Block Inheritance**. Group Policy Object links that are set to **Enforced** are always applied, however, and they can't be blocked. For more information, see Group Policy Basics – Part 2: Understanding Which GPOs to Apply.

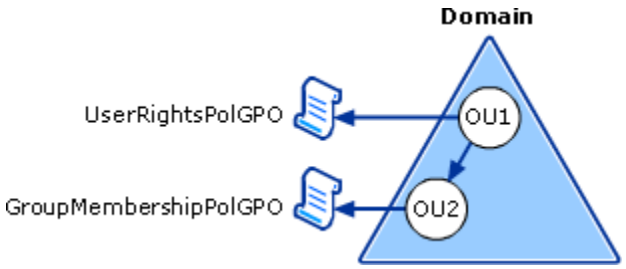
Security settings policy processing

In the context of Group Policy processing, security settings policy is processed in the following order.

1. During Group Policy processing, the Group Policy engine determines which security settings policies to apply.
2. If security settings policies exist in a GPO, Group Policy invokes the Security Settings client-side extension.
3. The Security Settings extension downloads the policy from the appropriate location such as a specific domain controller.
4. The Security Settings extension merges all security settings policies according to precedence rules. The processing is according to the Group Policy processing order of local, site, domain, and organizational unit (OU), as described earlier in the "Group Policy processing order" section. If multiple GPOs are in effect for a given device and there are no conflicting policies, then the policies are cumulative and are merged.

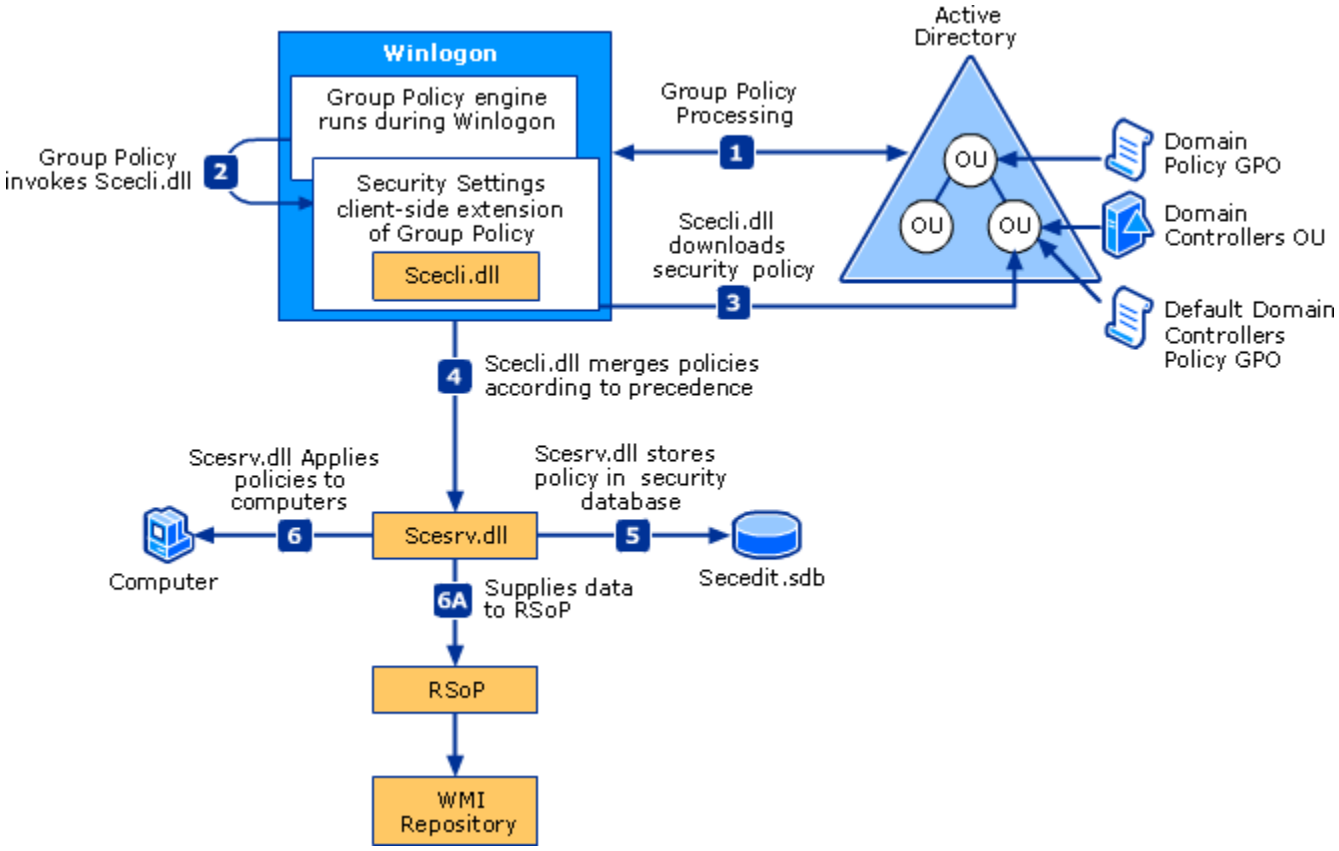
This example uses the Active Directory structure shown in the following figure. A given computer is a member of OU2, to which the **GroupMembershipPolGPO** GPO is linked. This computer is also subject to the **UserRightsPolGPO** GPO, which is linked to OU1, higher in the hierarchy. In this case, no conflicting policies exist so the device receives all of the policies contained in both the **UserRightsPolGPO** and the **GroupMembershipPolGPO** GPOs.

Multiple GPOs and Merging of Security Policy



5. The resultant security policies are stored in secedit.sdb, the security settings database. The security engine gets the security template files and imports them to secedit.sdb.
6. The security settings policies are applied to devices. The following figure illustrates the security settings policy processing.

Security Settings Policy Processing



Merging of security policies on domain controllers

Password policies, Kerberos, and some security options are only merged from GPOs that are linked at the root level on the domain. This merging is done to keep those settings synchronized across all domain controllers in the domain. The following security options are merged:

- Network Security: Force sign out when sign-in hours expire
- Accounts: Administrator account status
- Accounts: Guest account status
- Accounts: Rename administrator account
- Accounts: Rename guest account

Another mechanism exists that allows security policy changes made by administrators by using net accounts to be merged into the Default Domain Policy GPO. User rights changes that are made by using Local Security Authority (LSA) APIs are filtered into the Default Domain Controllers Policy GPO.

Special considerations for domain controllers

If an application is installed on a primary domain controller (PDC) with operations master role (also known as flexible single master operations or FSMO) and the application makes changes to user rights or password policy, these changes must be communicated to ensure that synchronization across domain controllers occurs. Scesrv.dll receives a notification of any changes made to the security account manager (SAM) and LSA that need to be synchronized across domain controllers and then incorporates the changes into the Default Domain Controller Policy GPO by using scecli.dll template modification APIs.

When security settings are applied

After you've edited the security settings policies, the settings are refreshed on the computers in the organizational unit linked to your Group Policy Object in the following instances:

- When a device is restarted.
- Every 90 minutes on a workstation or server and every 5 minutes on a domain controller. This refresh interval is configurable.
- By default, Security policy settings delivered by Group Policy are also applied every 16 hours (960 minutes) even if a GPO hasn't changed.

Persistence of security settings policy

Security settings can persist even if a setting is no longer defined in the policy that originally applied it.

Security settings might persist in the following cases:

- The setting hasn't been previously defined for the device.
- The setting is for a registry security object.
- The settings are for a file system security object.

All settings applied through local policy or through a Group Policy Object are stored in a local database on your computer. Whenever a security setting is modified, the computer saves the security setting value to the local database, which retains a history of all the settings that have been applied to the computer. If a policy first defines a security setting and then no longer defines that setting, then the setting takes on the previous value in the database. If a previous value doesn't exist in the database, then the setting doesn't revert to anything and remains defined as is. This behavior is sometimes referred to as "tattooing".

Registry and file security settings will maintain the values applied through Group Policy until that setting is set to other values.

Permissions required for policy to apply

Both Apply Group Policy and Read permissions are required to have the settings from a Group Policy Object apply to users or groups, and computers.

Filtering security policy

By default, all GPOs have Read and Apply Group Policy both Allowed for the Authenticated Users group. The Authenticated Users group includes both users and computers. Security settings policies are computer-based. To specify which client computers will or won't have a Group Policy Object applied to them, you can deny them either the Apply Group Policy or Read permission on that Group Policy Object. Changing these permissions allows you to limit the scope of the GPO to a specific set of computers within a site, domain, or OU.

Note

Do not use security policy filtering on a domain controller as this would prevent security policy from applying to it.

Migration of GPOs containing security settings

In some situations, you might want to migrate GPOs from one domain environment to another environment. The two most common scenarios are test-to-production migration, and production-to-production migration. The GPO copying process has implications for some types of security settings.

Data for a single GPO is stored in multiple locations and in various formats; some data is contained in Active Directory and other data is stored on the SYSVOL share on the domain controllers. Certain policy data might be valid in one domain but might be invalid in the domain to which the GPO is being copied. For example, Security Identifiers (SIDs) stored in security policy settings are often domain-specific. So copying GPOs isn't as simple as taking a folder and copying it from one device to another.

The following security policies can contain security principals and might require some more work to successfully move them from one domain to another.

- User rights assignment
- Restricted groups
- Services
- File system
- Registry
- The GPO DACL, if you choose to preserve it during a copy operation

To ensure that data is copied correctly, you can use Group Policy Management Console (GPMC). When there's a migration of a GPO from one domain to another, GPMC ensures that all relevant data is properly copied. GPMC also offers migration tables, which can be used to update domain-specific data to new values as part of the migration process. GPMC hides much of the complexity involved in the migrating GPO operations, and it provides simple and reliable mechanisms for performing operations such as copy and backup of GPOs.

In this section

Topic	Description
Administer security policy settings	This article discusses different methods to administer security policy settings on a local device or throughout a small- or medium-sized organization.
Configure security policy settings	Describes steps to configure a security policy setting on the local device, on a domain-joined device, and on a domain controller.

Topic	Description
Security policy settings reference	This reference of security settings provides information about how to implement and manage security policies, including setting options and security considerations.

Microsoft Intune vs GPOs

Microsoft Intune, part of Microsoft's Enterprise Mobility + Security (EMS) suite, is not a direct replacement for Group Policy Objects (GPOs) but rather a different approach to device and application management. Intune is designed primarily for managing mobile devices and applications, and it extends management capabilities to a wider range of devices, including those not running Windows.

Intune does not directly apply traditional Group Policy settings. Instead, it uses a different set of configuration profiles and policies that are more suited to modern mobile device management (MDM) and mobile application management (MAM). These policies allow administrators to control features on mobile devices and applications, enforce security settings, and manage data protection.

Key differences between Intune and GPOs include:

1. **Platform Support:** Intune supports a variety of platforms, including iOS, Android, and Windows, whereas GPOs are specific to Windows environments.
2. **Management Scope:** GPOs are designed for in-depth management of Windows desktops and servers within an Active Directory domain. Intune, on the other hand, is more focused on broad device management across different platforms and user scenarios, including remote and mobile workforces.
3. **Cloud-Based:** Intune is a cloud-based service, making it accessible and manageable from anywhere, whereas GPOs typically require access to the on-premises Active Directory infrastructure.
4. **Modern Management:** Intune aligns with the modern management approach, which is more about managing the user's identity and access across devices and applications, rather than managing the devices themselves in detail.

While Intune may not directly apply GPOs, it offers a modern alternative for organizations moving towards cloud-based management and dealing with a diverse array of devices and operating systems.

Dcgpofix

In this article

Applies To: Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012, Windows 8

Recreates the default Group Policy Objects (GPOs) for a domain. For examples of how this command can be used, see Examples.

Syntax

DCGPOFix [/ignoreschema] [/target: {Domain | DC | Both}] [/?]

Parameters

Parameter	Description
/ignoreschema	Ignores the version of the Active Directory® schema mc when you run this command. Otherwise, the command only works on the same schema version as the Windows version in which the command was shipped.
/target {Domain | DC | Both}	Specifies which GPO to restore. You can restore the Default Domain Policy GPO, the Default Domain Controllers GPO, or both.
/?	Displays Help at the command prompt.

Remarks

- The **dcgpofix** command is available in Windows Server 2008 R2 and Windows Server 2008, except on Server Core installations.
- Although the Group Policy Management Console (GPMC) is distributed with Windows Server 2008 R2 and Windows Server 2008, you must install Group Policy Management as a feature through Server Manager.

Examples

Restore the Default Domain Policy GPO to its original state. You will lose any changes that you have made to this GPO. As a best practice, you should configure the Default Domain Policy GPO only to manage the default Account Policies settings, Password Policy, Account Lockout Policy, and Kerberos Policy. In this example, you ignore the version of the Active Directory schema so that the **dcgpofix** command is not limited to same schema as the Windows version in which the command was shipped.

dcgpofix /ignoreschema /target:Domain

Restore the Default Domain Controllers Policy GPO to its original state. You will lose any changes that you have made to this GPO. As a best practice, you should configure the Default Domain Controllers Policy GPO only to set user rights and audit policies. In this example, you ignore the version of the Active Directory schema so that the **dcgpofix** command is not limited to same schema as the Windows version in which the command was shipped.

dcgpofix /ignoreschema /target:DC

Group Policy Client Side Extension List

So I was on a customer site, troubleshooting a Group policy Client Side extension issue and could not quite figure out all of the Client side extensions that were in use just by GUID. I was reviewing the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions and there were loads of extensions that was unsure about what they were. Some had no information about them held in the registry (As far as I could see anyway :))

So I said to myself, Mark (which is indeed my name ;) wouldnt it be nice to have a list of as many GPO extensions as possible, so that if I run into this situation again, I can resolve all the GPO CSE extensions using a quick reference list. So as I searched the internet, there does not seem to be a list of all Client Side extensions and their functions (There are a few scattered across MSDN or Microsoft.com or Technet). So, here we go with mine.. I will update this list as I go along. Feel free to tell me any more that you want to add to this list, or indeed, correct my list :)

GUID:	Component
{00000000-0000-0000-0000-000000000000}	Core GPO Engine
{0E28E245-9368-4853-AD84-6DA3BA35BB75}	Preference CSE GUID Environment Variables
{0F6B957D-509E-11D1-A7CC-0000F87571E3}	Tool Extension GUID (Computer Policy Settings)
{0F6B957E-509E-11D1-A7CC-0000F87571E3}	Tool Extension GUID (User Policy Settings) - Restrict Run
{1612b55c-243c-48dd-a449-ffc097b19776}	Preference Tool CSE GUID Data Sources
{17D89FEC-5C44-4972-B12D-241CAEF74509}	Preference CSE GUID Local users and groups
{1A6364EB-776B-4120-ADE1-B63A406A76B5}	Preference CSE GUID Devices
{1b767e9a-7be4-4d35-85c1-2e174a7ba951}	Preference Tool CSE GUID Devices
{25537BA6-77A8-11D2-9B6C-0000F8080861}	Folder Redirection
{2EA1A81B-48E5-45E9-8BB7-A6E3AC170006}	Preference Tool CSE GUID Drives
{3060E8CE-7020-11D2-842D-00C04FA372D4}	Remote Installation Services.
{35141B6B-498A-4CC7-AD59-CEF93D89B2CE}	Preference Tool CSE GUID Environment Variables
{35378EAC-683F-11D2-A89A-00C04FBBCFA2	Registry Settings
{3610EDA5-77EF-11D2-8DC5-00C04FA31A66}	Microsoft Disk Quota
{3A0DBA37-F8B2-4356-83DE-3E90BD5C261F}	Preference CSE GUID Network Options
{3BAE7E51-E3F4-41D0-853D-9BB9FD47605F}	Preference Tool CSE GUID Files
{3BFAE46A-7F3A-467B-8CEA-6AA34DC71F53}	Preference Tool CSE GUID Folder Options
{3EC4E9D3-714D-471F-88DC-4DD4471AAB47}	Preference Tool CSE GUID Folders
{40B66650-4972-11D1-A7CA-0000F87571E3}	Scripts (Logon/Logoff) Run Restriction
{42B5FAAE-6536-11d2-AE5A-0000F87571E3}	ProcessScriptsGroupPolicy
{47BA4403-1AA0-47F6-BDC5-298F96D1C2E3}	Print Policy in PolicyMaker
{4CFB60C1-FAA6-47f1-89AA-0B18730C9FD3}	Internet Explorer Zonemapping
{516FC620-5D34-4B08-8165-6A06B623EDEB}	Preference Tool CSE GUID Ini Files
{53D6AB1D-2488-11D1-A28C-00C04FB94F17}	Certificates Run Restriction
{5794DAFD-BE60-433f-88A2-1A31939AC01F}	Preference CSE GUID Drives
{5C935941-A954-4F7C-B507-885941ECE5C4}	Preference Tool CSE GUID Internet Settings
{6232C319-91AC-4931-9385-E70C2B099F0E}	Group Policy Folders
{6232C319-91AC-4931-9385-E70C2B099F0E}	Preference CSE GUID Folders

{6A4C88C6-C502-4f74-8F60-2CB23EDC24E2}	Preference CSE GUID Network Shares
{7150F9BF-48AD-4da4-A49C-29EF4A8369BA}	Preference CSE GUID Files
{728EE579-943C-4519-9EF7-AB56765798ED}	Preference CSE GUID Data Sources
{74EE6C03-5363-4554-B161-627540339CAB}	Preference CSE GUID Ini Files
{79F92669-4224-476c-9C5C-6EFB4D87DF4A}	Preference Tool CSE GUID Local users and groups
{7B849a69-220F-451E-B3FE-2CB811AF94AE}	Internet Explorer User Accelerators/PolicyMaker
{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}	Computer Restricted Groups
{827D319E-6EAC-11D2-A4EA-00C04F79F83A}	Security
{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}	Folder Redirection
{8A28E2C5-8D06-49A4-A08C-632DAA493E17}	Deployed Printer Connections
{91FBB303-0CD5-4055-BF42-E512A681B325}	Preference CSE GUID Services
{942A8E4F-A261-11D1-A760-00C04FB9603F}	Software Installation (Computers).
{949FB894-E883-42C6-88C1-29169720E8CA}	Preference Tool CSE GUID Network Options
{9AD2BAFE-63B4-4883-A08C-C3C6196BCAFD}	Preference Tool CSE GUID Power Options
{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B]	Internet Explorer Maintenance policy processing
{A3F3E39B-5D83-4940-B954-28315B82F0A8}	Preference CSE GUID Folder Options
{A8C42CEA-CDB8-4388-97F4-5831F933DA84}	Preference Tool CSE GUID Printers
{AADCED64-746C-4633-A97C-D61349046527}	Preference CSE GUID Scheduled Tasks
{B087BE9D-ED37-454f-AF9C-04291E351182}	Preference CSE GUID Registry
{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A]	EFS Recovery
{B587E2B1-4D59-4e7e-AED9-22B9DF11D053}	802.3 Group Policy
{B9CCA4DE-E2B9-4CBD-BF7D-11B6EBFBDDF7}	Preference Tool CSE GUID Regional Options
{BACF5C8A-A3C7-11D1-A760-00C04FB9603F}	Software Installation (Users) Run Restriction
{BC75B1ED-5833-4858-9BB8-CBF0B166DF9D}	Preference CSE GUID Printers
{BEE07A6A-EC9F-4659-B8C9-0B1937907C83}	Preference Tool CSE GUID Registry
{BFCBBEB0-9DF4-4c0c-A728-434EA66A0373}	Preference Tool CSE GUID Network Shares
{C418DD9D-0D14-4efb-8FBF-CFE535C8FAC7}	Preference CSE GUID Shortcuts
{C631DF4C-088F-4156-B058-4375F0853CD8}	Microsoft Offline Files
{C6DC5466-785A-11D2-84D0-00C04FB169F7]	Application Management
{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}	Preference Tool CSE GUID Scheduled Tasks
{CC5746A9-9B74-4be5-AE2E-64379C86E0E4}	Preference Tool CSE GUID Services
{cdeafc3d-948d-49dd-ab12-e578ba4af7aa}	TCPIP
{CEFFA6E2-E3BD-421B-852C-6F6A79A59BC1}	Preference Tool CSE GUID Shortcuts
{CF7639F3-ABA2-41DB-97F2-81E2C5DBFC5D}	Internet Explorer Machine Accelerators
{CF7639F3-ABA2-41DB-97F2-81E2C5DBFC5D}	Policy Maker
{CF848D48-888D-4F45-B530-6A201E62A605}	Preference Tool CSE GUID Start Menu
{D02B1F72-3407-48AE-BA88-E8213C6761F1}	Tool Extension GUID (Computer Policy Settings)
{D02B1F73-3407-48AE-BA88-E8213C6761F1}	Tool Extension GUID (User Policy Settings)
{e437bc1c-aa7d-11d2-a382-00c04f991e27]	IP Security
{E47248BA-94CC-49C4-BBB5-9EB7F05183D0}	Preference CSE GUID Internet Settings
{E4F48E54-F38D-4884-BFB9-D4D2E5729C18}	Preference CSE GUID Start Menu
{E5094040-C46C-4115-B030-04FB2E545B00}	Preference CSE GUID Regional Options
{E62688F0-25FD-4c90-BFF5-F508B9D2E31F}	Preference CSE GUID Power Options
{F0DB2806-FD46-45B7-81BD-AA3744B32765}	Policy Maker
{F17E8B5B-78F2-49A6-8933-7B767EDA5B41}	Policy Maker

{F27A6DA8-D22B-4179-A042-3D715F9E75B5}	Policy Maker
{f3ccc681-b74c-4060-9f26-cd84525dca2a}	Audit Policy Configuration
{F581DAE7-8064-444A-AEB3-1875662A61CE}	Policy Maker
{F648C781-42C9-4ED4-BB24-AEB8853701D0}	Policy Maker
{F6E72D5A-6ED3-43D9-9710-4440455F6934}	Policy Maker
{F9C77450-3A41-477E-9310-9ACD617BD9E3}	Group Policy Applications
{FB2CA36D-0B40-4307-821B-A13B252DE56C}	Enterprise QoS
{FC715823-C5FB-11D1-9EEF-00A0C90347FF}	Internet Explorer Maintenance Extension protocol
{FD2D917B-6519-4BF7-8403-456C0C64312F}	Policy Maker
{FFC64763-70D2-45BC-8DEE-7ACAF1BA7F89}	Policy Maker

Table 4-4. Group Policy Client-Side Extensions

Client-Side Extension	CSE DLL	GUID
Wireless Group Policy	Wlgpclnt.dll	{0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63}
Group Policy Environment	Gpprefcl.dll	{0E28E245-9368-4853-AD84-6DA3BA35BB75}
Group Policy Local Users and Groups	Gpprefcl.dll	{17D89FEC-5C44-4972-B12D-241CAEF74509}

Client-Side Extension	CSE DLL	GUID
Group Policy Device Settings	Gpprefcl.dll	{1A6364EB-776B-4120-ADE1-B63A406A76B5}
Folder Restriction	Fdeploy.dll	{25537BA6-77A8-11D2-9B6C-0000F8080861}
Microsoft Disk Quota	Diskquota.dll	{3610eda5-77ef-11d2-8dc5-00c04fa31a66}
Group Policy Network Options	Gpprefcl.dll	{3A0DBA37-F8B2-4356-83DE-3E90BD5C261F}
QoS Packet Scheduler	Gptext.dll	{426031c0-0b47-4852-b0ca-ac3d37bfcb39}
Scripts	Gpscript.dll	{42B5FAAE-6536-11d2-AE5A-0000F87571E3}
Internet Explorer Zonemapping	Iedkcs32.dll	{4CFB60C1-FAA6-47f1-89AA-0B18730C9FD3}
Group Policy Drive Maps	Gpprefcl.dll	{5794DAFD-BE60-433f-88A2-1A31939AC01F}
Group Policy Folders	Gpprefcl.dll	{6232C319-91AC-4931-9385-E70C2B099F0E}
Group Policy Network Shares	Gpprefcl.dll	{6A4C88C6-C502-4f74-8F60-2CB23EDC24E2}
Group Policy Files	Gpprefcl.dll	{7150F9BF-48AD-4da4-A49C-29EF4A8369BA}
Group Policy Data Sources	Gpprefcl.dll	{728EE579-943C-4519-9EF7-AB56765798ED}
Group Policy Ini Files	Gpprefcl.dll	{74EE6C03-5363-4554-B161-627540339CAB}
Windows Search Group Policy Extension	Srchadmin.dll	{7933F41E-56F8-41d6-A31C-4148A711EE93}
Security	Scecli.dll	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Deployed Printer Connections	Gpprnext.dll	{8A28E2C5-8D06-49A4-A08C-632DAA493E17}
Group Policy Services	Gpprefcl.dll	{91FBB303-0CD5-4055-BF42-E512A681B325}
Internet Explorer Branding	Iedkcs32.dll	{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
Group Policy Folder Options	Gpprefcl.dll	{A3F3E39B-5D83-4940-B954-28315B82F0A8}
Group Policy Scheduled Tasks	Gpprefcl.dll	{AADCED64-746C-4633-A97C-D61349046527}
Group Policy Registry	Gpprefcl.dll	{B087BE9D-ED37-454f-AF9C-04291E351182}
EFS Recovery	Scecli.dll	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
802.3 Group Policy	Dot3gpclnt.dll	{B587E2B1-4D59-4e7e-AED9-22B9DF11D053}
Group Policy Printers	Gpprefcl.dll	{BC75B1ED-5833-4858-9BB8-CBF0B166DF9D}
Group Policy Shortcuts	Gpprefcl.dll	{C418DD9D-0D14-4efb-8FBF-CFE535C8FAC7}
Microsoft Offline Files	Cscobj.dll	{C631DF4C-088F-4156-B058-4375F0853CD8}
Software Installation	Appmgmts.dll	{c6dc5466-785a-11d2-84d0-00c04fb169f7}
IP Security	Polstore.dll	{e437bc1c-aa7d-11d2-a382-00c04f991e27}

Client-Side Extension	CSE DLL	GUID
Group Policy Internet Settings	Gpprefcl.dll	{E47248BA-94CC-49c4-BBB5-9EB7F05183D0}
Group Policy Start Menu Settings	Gpprefcl.dll	{E4F48E54-F38D-4884-BFB9-D4D2E5729C18}
Group Policy Regional Options	Gpprefcl.dll	{E5094040-C46C-4115-B030-04FB2E545B00}
Group Policy Power Options	Gpprefcl.dll	{E62688F0-25FD-4c90-BFF5-F508B9D2E31F}
Group Policy Applications	Gpprefcl.dll	{F9C77450-3A41-477E-9310-9ACD617BD9E3}
Enterprise QoS	Gptext.dll	{FB2CA36D-0B40-4307-821B-A13B252DE56C}

He has shown you, O mortal, what is good.

And what does the Lord require of you?

To act justly and to love mercy

and to walk humbly with your God.

Group Policy Survival Guide

This is a list of Group Policy resources. You can add resources you find useful, and/or rearrange the ones that are here, for example, by adding new sections.

Table of Contents

- Troubleshooting
- Download
- Tools
- Blogs
- Forums
- Useful KBs
- Scripts
- Hands On Lab
- Books
- Trainings
- Videos
- See Also

What's going on

- Windows Server 2012 – The New and Improved Group Policy Management Console
- What's new in Group Policy in Windows Server 2012 R2
- What's new in Group Policy in Windows Server 2012

Concepts & How To

- Group Policy for Beginners
- Controlling the Scope of Group Policy Objects using GPMC
- GPMC How To...
- Group Policy Preferences Overview
- Group Policy Preferences Frequently Asked Questions
- How to apply Group Policy objects to Terminal Services servers

- Group Policy processing and precedence
- Group Policy and Logon Impact: Foreground vs. background processing & Synchronous vs. asynchronous processing
- Group Policy Basics – Part 1: Understanding the Structure of a Group Policy Object
- Group Policy Basics – Part 2: Understanding Which GPOs to Apply
- Group Policy Basics – Part 3: How Clients Process GPOs

Planning & Deployment

- Planning and Deploying Group Policy
- Group Policy Design Best Practices
- Deploying Group Policy Using Windows Vista
- Optimizing Group Policy Performance
- Windows Server 2003 Deployment Kit, Designing a Managed Environment Book
- Planning a Managed Environment
- Designing a Group Policy Infrastructure
- Staging Group Policy Deployments
- Deploying Security Policy
- Deploying a Managed Software Environment

Technical References

- Core Group Policy Technical Reference
    - Group Policy Search
    - What is Core Group Policy?
    - How Core Group Policy Works
    - Core Group Policy Tools and Settings
- Group Policy Components
    - Administrative Templates Extension Technical Reference
    - Group Policy Software Installation Extension Technical Reference

- Security Settings Extension Technical Reference
- IPSec Policy Extension Technical Reference
- Software Restriction Policies Technical Reference
- Scripts Extension Technical Reference
- Wireless Network Policies Extension Technical Reference
- Folder Redirection Extension Technical Reference
- Internet Explorer Maintenance Extension Technical Reference
- Remote Installation Services Extension Technical Reference

- Group Policy Settings Reference
  - Group Policy Settings Reference for Windows and Windows Server
  - Windows Internet Explorer 8
  - Windows Internet Explorer 9
  - Windows Internet Explorer 10
  - Windows Defender
- Group Policy ADMX Syntax Reference Guide
  - Group Policy ADMX Syntax Reference Guide
- Group Policy Management Console Reference
  - Group Policy Management Console icons reference
- Group Policy Preferences Guide
  - Group Policy Preferences Getting Started Guide
  - Using Group Policy Preferences
  - GP Policy vs. Preference vs. GP preferences
  - Windows 7: Group Policy Preferences
  - Geek of All Trades: GPPs for the GPP-less
  - Expanded Control with Group Policy Preferences

- Group Policy Preferences: Get Them Running Today!

Documents

- Group Policy for Beginners
- Group Policy Settings Reference for Windows and Windows Server
- Windows Server 2012 Core Network Companion Guide: Group Policy Deployment
- Deploying VPN Connections by Using Windows Powershell and Group Policy

Troubleshooting

- TechNet Library: Troubleshooting Group Policy Using Event Logs
- TechNet Library: Troubleshooting Windows Server 2008 - Group Policy Events and Errors
- Application of Group Policy
- Group Policy Preprocessing (Active Directory)
- Group Policy Preprocessing (General)
- Group Policy Preprocessing (Networking)
- Group Policy Preprocessing (Security)
- Group Policy Preprocessing (WMI)
- Group Policy Reporting
- Group Policy Service
- Software Installation Processing
- Group Policy Scripts Processing
- Group Policy Registry Processing
- KB2002507: Information about Group Policy Preferences Events
- TechNet Library: Group Policy Troubleshooting
- Fixing Group Policy networking issues
- Fixing Group Policy processing issues
- Fixing Group Policy Scoping issues

- Fixing Group Policy structural issues
- Fixing Administrative Template policy setting problem
- Fixing Security Settings Problems
- Fixing Scripts policy settings problems
- Fixing Software Installation policy setting problems
- Fixing Folder Redirection policy setting problems
- Fixing Disk Quota extension problems
- Fixing Group Policy problems by using log files
- TechNet Magazine: Your Guide to Group Policy Troubleshooting

Download

- Group Policy Management Console with Service Pack 1
- Group Policy Preference Client Side Extensions
    - Windows XP x32 Edition
    - Windows XP x64 Edition
    - Windows Server 2003 x32 Edition
    - Windows Server 2003 x64 Edition
    - Windows Vista x32 Edition
    - Windows Vista x64 Edition
    - Hotfix Rollup: May 2010
- Administrative Templates
    - Administrative Templates (ADMX) for Windows Server 2008
    - Administrative Templates (ADMX) for Windows Server 2008 R2 and Windows 7
    - Administrative Templates (.admx) for Windows 8 and Windows Server 2012
    - Administrative Templates (.admx) for Windows 8.1 Update and Windows Server 2012 R2 Update
    - Administrative Templates (.ADMX) for Windows 10

- Group Policy ADM Files
- Administrative Templates (ADMX) for Internet Explorer 9
- Administrative Templates (ADMX) for Internet Explorer 10
- Administrative Templates (ADMX) for Internet Explorer 11
- Office 2007 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool version 2.0
- Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool
- Microsoft Desktop Optimization Pack Group Policy Administrative Templates
- Collection of Administrative Templates

- Starter Group Policy Objects (GPOs)
- Recommended Updates for Group Policy in Windows Client and Server Products

Tools

- Group Policy Management Console (GPMC): A new and comprehensive administrative tool for Group Policy management. GPMC integrates the existing Group Policy functionality of the property pages on the Active Directory administrative tools into a single, unified console dedicated to Group Policy management tasks; GPMC also expands management capabilities with new features.
- Gpresult: A tool that displays the Resultant Set of Policy (RSoP) information for a remote user and computer.
- Gpupdate: A tool that you can use to manually update any changes that are made to group policies (some changes can be made immediately.
- Gpotool: A tool that you can use to check the health of the Group Policy objects on domain controllers.
- Recreatedefpol.exe: A tool developed to restore the Default Domain policies in case of accidental deletion for Windows 2000. For the Windows Server 2003, please use Dcgpofix.exe instead (included in Windows Server 2003).
- Group Policy Inventory (GPInventory.exe): A tool allows administrators to collect Group Policy and other information from any number of computers in their network by

running multiple Resultant Set of User Policy (RSOP) or Windows Management Instrumentation (WMI) queries. The query results can be exported to either an XML or a text file, and can be analyzed in Excel.

- Group Policy Search : Web app (hosted on Azure) allowing you to search all group policy settings available for Windows, Office and IE. E.G. search 'Wallpaper' to find all settings that relate to wallpaper
  Windows Phone App - Search for Group Policy Search in the store or download the XAP and install manually
- Search Connector for Windows Explorer - Search Group Policy Settings straight from Windows Explorer's search bar. Unfortunately, this points to the old site URL. Just open the OSDX file in notepad and change the URL to "http://gpsearch.azurewebsites.net/gps/rss.ashx?search={searchTerms}"
- Group Policy Log View : A utility that you can use to export Group Policy event data from the system and operational log into a text, HTML, or XML files. The supported operating system is Windows Vista.
- Policy Reporter V4 : A free software from SysPro which formats the log provided in %systemRoot%\Debug\UserMode to give a more meaningful display. This latest version also displays the logs created when processing Preferences. It provides a tree structure on the left which shows major events reported in the Log. Selecting an entry in the tree structure displays that section of the log in the view window.
- Free GPOGuy tools A lot of interesting Toos like: command line remote GPO refresh, Group Policy Software Installation Viewer Utility, WMI Filter Validation Utility etc.

Blogs

- Group Policy Team Blog
- Blog posts tagged with Group Policy in AskDS
- Jeremy's GP Blog
- Group Policy Central

Forums

- Group Policy Forum

Useful KBs

- Userenv errors occur and events are logged after you apply Group Policy to computers that are running Windows Server 2003, Windows XP, or Windows 2000
- Group Policy Slow Link Detection Using Windows Vista and Server 2008
- Windows 7 Clients intermittently fail to apply group policy at startup
- Default Behavior for Group Policy Extensions with Slow Link
- Troubleshooting Group Policy Client-Side Extension Behavior

Scripts

- Group Policy Cmdlets in Windows PowerShell
- Learn About Scripting for Group Policy (Hey, Scripting Guy!)
- Blog posts tagged with Scripting in Group Policy Team blog
- Scripting Group Policy Tasks using GPMC
- TechNet Virtual Lab: Applying Group Policy
- TechNet Virtual Lab: MDOP: Advanced Group Policy Management (APGM)
- TechNet Virtual Lab: Managing a Domain Environment More Effectively
- TechNet Virtual Lab: MDOP: User State Virtualization (USV)
- TechNet Virtual Lab: Managing Internet Explorer 8 in the Enterprise
- TechNet Virtual Lab: Fine Grained Password Settings in Windows Server 2008 Beta 3
- Group Policy Management Console Scripting Samples

Hands On Lab

- TechNet Virtual Lab: Applying Group Policy
- TechNet Virtual Lab: MDOP: Advanced Group Policy Management (APGM)
- TechNet Virtual Lab: Managing a Domain Environment More Effectively
- TechNet Virtual Lab: MDOP: User State Virtualization (USV)
- TechNet Virtual Lab: Managing Internet Explorer 8 in the Enterprise
- TechNet Virtual Lab: Fine Grained Password Settings in Windows Server 2008 Beta 3

Books

- Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista
- Windows Group Policy Administrator's Pocket Consultant
- Microsoft Windows Group Policy Guide
- Group Policy: Fundamentals, Security, and the Managed Desktop

Trainings

- Online Training
    - Course 6719: Troubleshooting Group Policy Issues in Windows Server 2008
    - Course 6178: Designing AD DS Group Policy in Windows Server 2008
    - Course 6715: Configuring User Environments by Using Group Policy in Windows Server 2008
    - Course 6716: Implementing Security by Using Group Policy in Windows Server 2008
    - Course 6714: Configuring Group Policy Objects in Windows Server 2008
- Classroom Training
    - Course 50255A: Managing, Maintaining, and Securing Your Networks Through Group Policy

Videos

- Administration and Configuration
    - Windows Server 2008 R2 and Windows 7 Group Policy Changes
    - What's new in Group Policy for Windows 7?
    - Group Policy in Windows Vista
    - Review Group Policy Features
    - Configuring Group Policy
    - Using Group Policy Preferences
    - Using Group Policy to set default printers in Windows 7
    - Power Management and Troubleshooting Group Policy

- Understanding Group Policy (Part 1 of 3)
- Understanding Group Policy (Part 2of 3)
- Understanding Group Policy (Part 3 of 3)
- Group Policy Preferences, Templates and Scripting
- Improving Desktop Security and Deployment (Part 6 of 7): Group Policy in Windows Vista
- Microsoft's Solutions for Windows Vista Management

- How do I series
  - How do I: Configure The Central ADMX Store
  - How do I: Windows 7/Server 08 R2 Software Restriction Policies
  - How do I: Windows Server 2008 R2 Quick Look - Group Policy Management
  - How do I: Use Group Policy Preferences to Manage Windows Vista Computers?
  - How do I: Using Group Policy in Windows Vista and Windows Server 2008?
  - How do I: Create a group policy to manage Windows Phone devices with System Center Mobile Device Manager 2008?
  - How do I: Configuring and Using Advanced Group Policy Management
- Troubleshooting
  - Troubleshooting Group Policy
- Networking Isolation
  - Network Isolation Using Group Policy and IPsec (Part 1 of 3)
  - Network Isolation Using Group Policy and IPsec (Part 2 of 3)
  - Network Isolation Using Group Policy and IPsec (Part 3 of 3)
- Advanced Group Policy Management
  - Windows Server 2008 R2 Quick Look - Group Policy Management
  - A tour of Advanced Group Policy Management
  - Microsoft Advanced Group Policy Management

See Also

- Wiki: List of Technologies and Related Topics
- Wiki: Survival Guides Portal

Now all has been heard;

here is the conclusion of the matter:

Fear God and keep his commandments,

for this is the duty of all mankind.

For God will bring every deed into judgment,

including every hidden thing,

whether it is good or evil.

Slow Links and GPOs

You also have control over which major components of the GPO are processed over slow connection links. Some GPO components are always processed, regardless of the connection speed:

■ Administrative template settings
■ Security policies

The following are other settings that are processed over slow connection links by default but can be configured to not be processed over slow links:

■ EFS Recovery policies
■ IP Security policies
■ Software restrictions policies
■ Wireless policies
■ Internet Explorer Maintenance policies

The following components of a GPO aren't processed over slow links by default but can be configured to be processed over slow connection links:

■ Application deployment
■ Logon/logoff scripts
■ Folder redirection

■ Disk quotas

If I speak in the tongues of men or of angels, but do not have love, I am only a resounding gong or a clanging cymbal. If I have the gift of prophecy and can fathom all mysteries and all knowledge, and if I have a faith that can move mountains, but do not have love, I am nothing. If I give all I possess to the poor and give over my body to hardship that I may boast, but do not have love, I gain nothing.

Love is patient, love is kind. It does not envy, it does not boast, it is not proud. It does not dishonor others, it is not self-seeking, it is not easily angered, it keeps no record of wrongs. Love does not delight in evil but rejoices with the truth. It always protects, always trusts, always hopes, always perseveres.