

Supporting Group Policy

Module 01: Group Policy Introduction



V1.0 Released: February 17, 2014

# What Is a Group Policy?

Group Policy allows you to setup users’ environments only once, and to rely on the operating system to enforce them thereafter.

Group Policy objects are different from profiles. A profile is a user environment setting that a user can change desktop settings, registry settings in **NTUser.dat** files, profiles directory, My Documents, or Favorites. You, as the administrator, manage and maintain Group Policy, an MMC hosted administrative tool used to set policy on groups of users and computers.

# What Is a Local Group Policy?

In Windows 2000/2003, group policy is typically discussed as part of Active Directory, but Local Group Policies are also available. As its name implies, it is stored on a local machine at **\systemroot\System32\GroupPolicy**. It can be useful if you only need to apply certain settings to a small number of Windows XP or Windows 2000 clients, or your clients are not members of a domain.

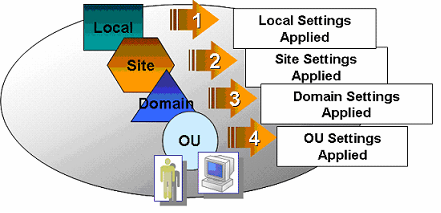
# Active Directory Structure and Group Policy

Group Policy uses the Active Directory structure (referred to in this course as the **Active Directory hierarchy**) as a **map** for applying specific GPOs to specific Users and Computers. Group Policy objects are **linked** to Active Directory container objects…Sites, Domains, or Organizational Units. These containers are collectively referred to as SDOU or SDOUs in Group Policy discussions, since any of these objects may have links to one or multiple GPOs. The location of the User or Computer account and the GPOs linked to the Site, Domain or Organizational Unit(s) in which those accounts reside determine what Policies are applied to the User or Computer.

It is important to note that GPOs cannot be linked from an object of objectClass=container. GPOs are linked only from objects of objectClass=Site, objectClass=domainDNS, and objectClass=OrganizationalUnit. These objects can contain other objects. For simplicity, these objects will be referred to as Group Policy containers when used generally in this course.

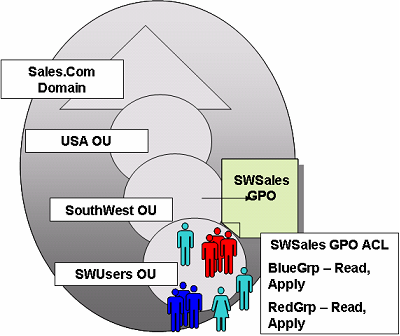
# What Is the Order of Group Policy Application?

Since Group Policies can be linked to Sites, Domains, or OUs, what determines the order of application? The local Group Policy object is applied first. Then site-linked Group Policy objects are applied in specified order, then domain-linked ones in specified order, and lastly organizational unit-linked Group Policy objects beginning at the highest (in Active Directory hierarchy) organizational unit containing the user or computer account and ending with the lowest (closest to the user or computer) organizational unit containing the user or computer. At each organizational unit, any Group Policy objects linked to it are applied in administratively specified order.



The order of application detailed in the previous paragraph (1. Local, 2. Site, 3. Domain, 4. Organizational Unit) is significant to the architecture of Active Directory, because by default, policy applied later overwrites policy applied earlier for each setting that is either **Enabled** or **Disabled**. Settings that are not configured do not overwrite anything — any **Enabled** or **Disabled** setting applied earlier is allowed to persist.

This is the default behavior for policy application. Mechanisms do exist that let you either force or prevent Group Policy objects from affecting groups of users or computers. The most powerful mechanisms for avoiding the default behavior are the **No Override** and **Block Policy Inheritance** settings. These settings can be configured via the GPO properties. It is best to minimize the use of these. What happens if these two settings appear to conflict? For example: an Administrator at the OU level could set the **Block Inheritance** flag for that OU, which would prevent Policies from above applying to accounts in that OU or in child OUs. However, if the Domain or Enterprise Administrator has set the **No Override** flag on a GPO, this would trump the Block Inheritance setting at the OU level.



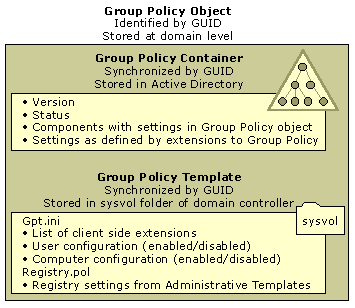
In order for a GPO to apply to a given user or computer, that user or computer must have both **Read** and **Apply Group Policy** permissions on the GPO. By default, Authenticated Users have both Apply Group Policy and Read permissions set to Allow. Both of these permissions are managed together as a single unit by using Security Filtering in Group Policy Management Console (GPMC).

To set the permissions for a given GPO:

1. Right click the OU and select **Properties**.
2. Select the **Group Policy** tab.
3. Select the correct Group Policy and click the **Properties** button.
4. Select the **Security** tab.

# Where Are GPOs Stored?

Domain Group Policy objects store Group Policy information in two locations: a **Group Policy container** and a **Group Policy template**. They are named with a globally unique identifier (GUID), which is used to keep them synchronized.



## Group Policy Container

The Group Policy container, located under cn=system, is an Active Directory storage area for Group Policy object properties; it includes both computer and user Group Policy information. The Group Policy container has the following properties:

* **Version Information**  
  This makes sure that the information is synchronized with the Group Policy template information.
* **Status Information**  
  This indicates whether the Group Policy object is enabled or disabled.
* **Components with Settings in GPO**  
  List of components (extensions) that have settings in the Group Policy object.
* **Policy Settings as Defined by the Extension Snap-ins**  
  For example, the Group Policy container stores information used by the Software Installation snap-in to describe the status of the software available for installation. This data repository contains data for all applications, interfaces, and APIs that provide for application publishing and assigning.

## Group Policy Template

Group Policy objects also store Group Policy information in a folder structure called the Group Policy template that is located in the System Volume folder of domain controllers (**Sysvol**) in the \Policies subfolder. The Group Policy template is the container where Administrative Template–based policy settings, Security Settings, applications available for Software Installation, and script files are stored.

When you modify a Group Policy object, the directory name given to the Group Policy template is the GUID of the Group Policy object that you modify. For example, a Group Policy template folder might be named as shown in the following example:

**%systemroot%\sysvol\SYSVOL\www.Reskit.com\Policies\{47636445-af79-11d0-91fe-080036644603}**

A Group Policy snap-in can store data outside the Group Policy object; however, this requires that at least a link to the Group Policy object be stored either in a Group Policy container (Active Directory data store) or in a Group Policy template (file-type data stored on the **Sysvol** folder).

# Viewing and Reporting of Policy Settings

In order to properly implement, troubleshoot, and plan Group Policy, administrators need to be able to quickly view the settings in a GPO. When multiple GPOs apply to a given user or computer, they can contain conflicting policy settings. For most policy settings, the final value of the policy setting is set only by the highest precedent GPO that contains that setting. Resultant Set of Policy (RSoP) helps you understand and identify the final set of policy that is applied as well as settings that did not apply as a result of policy inheritance.

Specifically, Resultant Set of Policy helps you determine:

* The final value of the setting that is applied as a result of all the GPOs.
* The final GPO that set the value of this setting (also known as the winning GPO).
* Precedence details that show any other GPOs that attempted to set this setting and the value that each GPO attempted to set for that policy setting.

Group Policy Management Console, available as a separate download from the Microsoft Web site, addresses some common reporting requirements including the ability to document all the settings in a GPO to a file for printing or viewing. Users can either print the reports, or save them to a file as either HTML or XML.

# Delegating Administration of Group Policy

Organizations need to be able to delegate administration of Group Policy to other administrators who can take responsibility for a given OU, domain, or other container. Active Directory is designed to allow you to delegate control of portions of the directory service in managing aspects of Group Policy. The following areas can be delegated:

* **GPO delegation.** This includes permission to create GPOs in a domain or permission to edit an existing GPO. Note that having permission to edit a GPO does not include any delegated rights on the GPO links.
* **Link delegation.** This includes permission to add, delete, or change links to GPOs. Note that having link delegation does not include any delegated rights on the GPO itself.
* **RSOP delegation.** This includes permission to run RSoP (in either planning or logging mode) on objects under a container.
* **WMI filter delegation.** This includes permission to create WMI filters or permission to edit an existing filter.

In GPMC, delegation is simplified because it manages the various Access Control Entries (ACEs) required for a task as a single bundle of permissions for the task. You can also use the Access Control List (ACL) editor to view or manage these permissions manually.

The underlying mechanism for achieving delegation is the application of the appropriate DACLs to GPOs and other objects in Active Directory. This mechanism is identical to using security groups to filter the application of GPOs to various users. You can also specify Group Policy to control who can use MMC snap-ins. For example, you can use Group Policy to manage the rights to create, configure, and use MMC consoles, and to control access to individual snap-ins.

# What Is User Group Policy Loopback Mode?

Group Policy applies to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. In some cases, this processing order may not be appropriate (for example, when you do not want applications that have been assigned or published to the users in their OU to be installed while they are logged on to the computers in some specific OU). With the Group Policy **loopback** support feature, you can specify two other ways to retrieve the list of GPOs for any user of the computers in this specific OU:

* **Merge Mode**In this mode, when the user logs on, the user's list of GPOs is gathered normally. Then the computer’s list of GPOs is gathered using the computer's location in Active Directory. The list of GPOs for the computer is then added to the end of the GPOs for the user. This causes the computer's GPOs to have higher precedence than the user's GPOs. In this example, the list of GPOs for the computer is added to the user's list.
* **Replace Mode**In this mode, the user's list of GPOs is not gathered. Only the list of GPOs based on the computer object is used.

# Group Policy Dependencies

Group Policy has several key dependencies. Domain-based Group Policy requires an Active Directory environment with DNS properly configured.

## Active Directory

Active Directory is the Windows 2000 Server and Windows Server 2003 directory service that stores information about all objects on the computer network and makes this information easy for administrators and users to find and apply. With Active Directory, users can gain access to resources anywhere on the network with a single logon. Similarly, administrators have a single point of administration for all objects on the network, which can be viewed in a hierarchical structure. In a network environment, Group Policy depends on Active Directory as the targeting framework that allows you to link GPOs to specific Active Directory containers such as sites, domains, or OUs.

In a stand-alone environment without Active Directory, you can use Local Group Policy objects to configure settings on individual computers.

## Domain Name System (DNS)

DNS is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

Group Policy application requires clients to access specified servers, including domain controllers and other servers such as share points and install points. Group Policy management also requires access to domain controllers. DNS is used to locate and identify these servers. In Windows 2000 Server and later Active Directory requires DNS support. If the network is functioning, but clients or consoles such as the Group Policy Object Editor or GPMC are unable to locate the servers, there might be a problem with your network's DNS system.

## Replication

Group Policy depends on other technologies in order to properly replicate between domain controllers in a network environment. A GPO is a virtual object stored in both Active Directory and the Sysvol of a domain controller. Property settings, stored in the Group Policy container, are replicated through Active Directory replication. Replication automatically copies the changes that originate on a writable directory partition replica to all other domain controllers that hold the same directory partition replica. More specifically, a destination domain controller pulls these changes from the source domain controller. Data settings, stored in the Sysvol as the Group Policy template, are replicated through the File Replication Service (FRS), which provides multi-master file replication for designated directory trees between designated servers running Windows Server 2003. The Group Policy container stores GPO properties, including information about version, GPO status, and a list of components that have settings in the GPO. The Group Policy template is a directory structure within the file system that stores Administrative Template-based policy settings, security settings, script files, and information regarding applications that are available for software installation. The Group Policy template is located in Sysvol in the \Policies sub-directory for its domain. GPOs are identified by their globally unique identifiers (GUIDs) and stored at the domain level. The settings from a GPO are only applied when the Group Policy container and Group Policy template are synchronized.

## DFS publishing

The Sysvol folder is shared on each domain controller and is accessible through the UNC path \\dcname.domainname\sysvol.

The Sysvol is also published as a domain-based Distributed File System (DFS) share. This allows clients to access the Sysvol by using the generic path \\*domainname*\sysvol. A request for a DFS referral for \\*domainname*\sysvol will always return a replica in the same Active Directory site as the client if one is available. This is the mechanism that the Group Policy client-side extensions use to retrieve a local copy of the Group Policy template information.