# Core Group Policy Processes an Interactions

## Group Policy Processing Rules

Settings that are applied later can override settings that are applied earlier. Group Policy settings are processed in the following order:

* **Local Group Policy object.** Each computer has exactly one Group Policy object that is stored locally. This processes for both computer and user Group Policy processing.
* **Site.** Processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the site in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.
* **Domain.**
* **Organizational units.** GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit are processed, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

To summarize, the Local GPO is processed first, and the organizational unit to which the computer or user belongs (the one that it is a direct member of) is processed last. All of this processing is subject to the following conditions:

* **WMI** or **Security Filtering** that has been applied to GPOs.
* Any domain-based GPO (not Local GPO) can be enforced by using the **Enforce** option so that its policies cannot be overwritten. Because an Enforced GPO is processed last, no other settings can write over the settings in that GPO. If you have more than one Enforced GPO, it's possible to set the same setting in each GPO to a different value, in which case, **the link order** of the GPOs determines which one contains the final settings.
* At any domain or organizational unit, Group Policy inheritance can be selectively designated as Block Inheritance. However, because enforced GPOs are always applied, and cannot be blocked, blocking inheritance does not prevent policy from Enforced GPOs from applying.

Every computer has a single Local GPO that is always processed regardless of whether the computer is part of a domain or is a stand-alone computer. The Local GPO can't be blocked by domain-based GPOs. However, settings in domain GPOs always take precedence since they are processed after the Local GPO.

## Targeting GPOs

The site, domain, and OU links from a GPO are used as the primary targeting principle for defining which computers and users should receive a GPO. Security filtering and WMI filtering can be used **to further reduce** the set of computers and users to which the GPO will apply. The Group Policy engine uses the following logic in processing GPOs: If a GPO is linked to a domain, site, or OU that applies to the user or computer, the Group Policy engine must then determine whether the GPO should be added to its GPO list for processing. A GPO is **blocked** from processing in the following circumstances:

* **The GPO is disabled.** You disable either or both the computer or user components of a GPO from its Policy Properties dialog box.
* **The computer or user does not have permission to read and apply the GPO.** You control permission to a GPO through **security filtering**, as explained in the following section.
* **A WMI filter applied to a GPO evaluates to false on the client computer.** A WMI filter must evaluate to true before the Group Policy engine will allow it to be processed, as explained in the following section.

## Security Filtering

Security filtering is a way of refining which users and computers will receive and apply the settings in a GPO. By using security filtering to specify that only certain security principals within a container where the GPO is linked apply the GPO, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer. Security filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO.

In order for the GPO to apply to a given user or computer, that user or computer must have both **Read** and **Apply Group Policy (AGP)** permissions on the GPO, either explicitly, or effectively though group membership.

By default, all GPOs have **Read** and **AGP** both **Allowed** for the Authenticated Users group. The Authenticated Users group includes both users and computers. However, administrators are members of Authenticated Users, which means that they will receive the settings in the GPO by default.

These permissions can be changed to limit the scope to a specific set of users, groups, or computers within the organizational unit, domain, or site. The Group Policy Management Console manages these permissions as a single unit, and displays the **security filtering** for the GPO on the GPO Scope tab. In GPMC, groups, users, and computers can be added or removed as security filters for each GPO.

## How Security Filtering is Processed

Before processing a GPO, the Group Policy engine checks the **Access Control List ACL** associated with the GPO. If an ACE(Access control entry) on a GPO denies a security principal to which the computer or user belongs, either the Apply Group Policy or Read permission, the Group Policy engine does not add the GPO to its list of GPOs to process. Additionally, an ACE on a GPO must allow the appropriate security principal both Apply Group Policy and Read permissions in order for the Group Policy engine to add the GPO to the GPO processing list.

If appropriate permissions are granted to the GPO, it is added to the list of GPOs to download.

In general, **Deny** ACEs should be avoided because you can achieve the same results by granting or not granting **Allow** permissions.

## Windows Management Instrumentation (WMI) Filtering

WMI makes **data** about a target computer available for administrative use. Such **data** can include hardware and software inventory, settings, and configuration information.

WMI filtering allows you to filter the application of a GPO by attaching a Windows Query Language query to a GPO. The queries can be written to query WMI for multiple items. If the query returns true for all queried items, then the GPO will be applied to the target user or computer.

The WMI filter is a separate object from the GPO in the directory. A WMI filter must be linked to a GPO in order to apply. Each GPO can have only one WMI filter; however the same WMI filter can be linked to multiple GPOs. WMI filters, like GPOs, are stored only in domains. A WMI filter and the GPO it is linked to must be in the same domain.

## How Windows Management Instrumentation (WMI) Filtering is Processed

If, after security filtering, appropriate permissions are granted to the GPO, it is added to the list of GPOs to download. Upon download, the **Group Policy engine** reads the **gPCWQLFilter** attribute in the Group Policy container to determine if a WMI filter is applied to the GPO. If so, the WMI filter, which contains one or more WQL statements, is evaluated. If the statement evaluates to true, then the GPO is processed. There are tradeoffs in using WMI filters because they can increase the amount of time it takes to process policy especially if the filter to be evaluated takes a long time to process.

## Windows Management Instrumentation (WMI)Filtering Scenarios

Sample uses of WMI filters include:

* Services. Computers where DHCP is turned on.
* Registry. Computers that have this registry key populated.
* Hardware inventory. Computers with a Pentium III processor.
* Software inventory. Computers with Visual Studio .NET installed.
* Hardware configuration. Computers with network interface cards (NICs) on interrupt level 3.
* Software configuration. Computers with multi-casting turned on.
* Associations. Computers that have any services dependent on Systems Network Architecture (SNA) service.

WMI filters are only available in domains that have at least one Windows Server 2003 domain controller.

## Initial Processing of Group Policy

Group Policy for computers is applied at computer startup. For users, Group Policy is applied when they log on. In Windows 2000, the processing of Group Policy is synchronous, which means that computer Group Policy is completed before the logon dialog box is presented, and user Group Policy is completed before the shell is active and available for the user to interact with it.

## Synchronous and Asynchronous Processing

Synchronous processes can be described as a series of processes where one process must finish running before the next one begins. Asynchronous processes, on the other hand, can run on different threads simultaneously because their outcome is independent of other processes.

You can change the default processing behavior by using a policy setting for each GPO so that processing is asynchronous instead of synchronous. For example, if the policy has been set to remove the **Run** command from the **Start** menu, it is possible under asynchronous processing that a user could logon prior to this policy taking effect, so the user would initially have access to this functionality.

How the Group Policy Engine Processes Client-Side Extensions (CSE)