



Purpose of this Document:

We receive many questions regarding Windows' processing of Group Policy Objects (GPOs), such as: what logic does Windows use when it processes GPOs; and which policy will take precedence for a certain user or computer belonging to a domain where multiple GPOs are linked to an Organizational Unit (OU), site or domain.

In the case of a large domain containing a large number of complex GPOs it is difficult, practically impossible, to answer the latter question due to the many interrelated logic paths used by Windows when it processes the GPOs.

The purpose of this document is to outline the main conditions that influence Windows when it processes and applies GPO policies.

GPO settings and options:

The following conditions combine together to influence Windows' processing of Group policies and determine which policies will ultimately win / take effect for a user or computer object:

1. The GPO's precedence in a list of GPOs linked to a Site, Domain, or OU

GPOs with a higher priority have a *higher precedence*, because they can overwrite the policies that are processed earlier in the list of GPOs.

2. The status of the GPO link to the Site, Domain, or OU

If a GPO link is *disabled*, the settings in the GPO will no longer apply to users or computers in the Site, Domain, or OU to which the GPO is linked. This includes objects in child Containers.

3. The *Block Policy Inheritance* flag for the Site, Domain, or OU

The *Block Policy Inheritance* flag blocks GPOs that apply higher in the Active Directory hierarchy of sites, domains, and OUs. It does not block GPOs if they have *No Override* enabled. Set on the Domain or OU, not on the GPO.

4. The *No Override* flag on the GPO Link

If the *No Override* flag is set it *enforces* policy inheritance. I.e. it forces all child policy containers to inherit the parent's policy, even if that policy conflicts with the child's policy and even if *Block Policy Inheritance* has been set for the child.

5. The GPO's *User Configuration Disabled* flag

Determines whether the GPO's *User Configuration* settings are active or disabled.

6. The GPO's *Computer Configuration Disabled* flag

Determines whether the GPO's *Computer Configuration* settings are active or disabled.



Miscellaneous Conditions:

In addition to the normal conditions above, several abnormal conditions can affect Windows processing of Group policies. SekChek has noticed that these unusual conditions occur surprisingly frequently, so we have summarised the most common conditions below:

- Configuration problems that prevent a GPO from being replicated across other DCs
- A GPO that does not exist on disk, even though it is defined in Active Directory
- Inappropriate NTFS permissions on the SYSVOL directory that prevent a GPO from being replicated

Useful Reference Documents:

You may find the following information sources useful:

- SekChek Local Report Database: The embedded Glossary document
- SekChek Local AD product specification document:
<http://www.sekchek.com/downloads/Product Specification - SekChek Local AD.pdf>
- Microsoft TechNet