Filtering the Scope of a GPO

By REDMOND\\markl

Archived: 2026-04-05 21:09:04 UTC

By default, a GPO affects all users and computers that are contained in the linked site, domain, or organizational unit. The administrator can further specify the computers and users that are affected by a GPO by using membership in security groups.

An administrator can add both computers and users to security groups. Then the administrator can specify which security groups are affected by the GPO by using the Access Control List (ACL) editor. To start the ACL editor, select the **Security** tab of the property page for the GPO. Then set access permissions using discretionary access control lists (DACLs) to allow or deny access to the GPO by specified groups. By changing the Access Control Entries (ACEs) within the DACL, the effect of any GPO can be modified to exclude or include the members of any security group. For more information about security groups, see How Security Groups are Used in Access Control.

To apply a GPO to a specific group, both the **Read** and **Apply Group Policy** ACEs are required. By default, all Authenticated Users have both these permissions set to **Allow**. Because everyone in an organizational unit is automatically an Authenticated User, the default behavior is for every GPO to apply to every Authenticated User. However, domain administrators, enterprise administrators, and the LocalSystem account already have full control permissions, by default, without the **Apply Group Policy** ACE. Therefore, because administrators are also Authenticated Users, they too, by default, will receive the policy settings in the GPO. This may not be the appropriate scenario.

There are different methods administrators can use to prevent a GPO policy from applying to a specific group (for example, to administrators). The recommended method is to remove (clear **Allow**) both the **Read** and **Apply Group Policy** ACEs for the group. Another method involves removing the **Apply Group Policy** ACE for Authenticated Users, and then explicitly granting the permission by checking **Allow** for the individual security groups that should receive the policy settings. You can also set the **Apply Group Policy** ACE to **Deny** for groups of users that do not require the policy.

> [!Warning]
> A **Deny** ACE setting for any group takes precedence over any **Allow** ACE granted to a user or computer as a result of membership in another group.

For more information about ACLs, DACLs, and ACEs, see Access Control.

In addition, by default, every computer receives a local GPO that contains registry policy settings and security-specific policy settings. This is useful for computers that are not members of a domain.

Administrators can also use WMI Filters for exception management. WMI Filters allow an administrator to specify a WMI-based query to filter the effect of a GPO. WMI Filters are written in WMI Query Language.

For more information, see Applying Group Policy.
