Delegating Administration of Group Policy

Updated: March 28, 2003

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Your Group Policy design will probably call for delegating certain Group Policy administrative tasks. Determining to what degree to centralize or distribute administrative control of Group Policy is one of the most important factors to consider when assessing the needs of your organization. In organizations that use a centralized administration model, an IT group provides services, makes decisions, and sets standards for the entire company. In organizations that use a distributed administration model, each business unit manages its own IT group.

You can delegate the following Group Policy tasks:

- Creating GPOs
- Managing individual GPOs (for example, granting Edit or Read access to a GPO)
- Performing the following tasks on sites, domains, and OUs:
    - Managing Group Policy links for a given site, domain, or OU
    - Performing Group Policy Modeling analyses for objects in that container (not applicable for sites)
    - Reading Group Policy Results data for objects in that container (not applicable for sites)
- Creating WMI filters
- Managing and editing individual WMI filters

Based on your organization's administrative model, you need to determine which aspects of configuration management can best be handled at the site, domain, and OU levels. You also need to determine how responsibilities at each site, domain, and OU level might be further subdivided among the available administrators or administrative groups at each level.

When deciding whether to delegate authority at the site, domain, or OU level, remember the following points:

- Authority delegated at the domain level affects all objects in the domain, if the permission is set to inherit to all child containers.

- Authority delegated at the OU level can affect either that OU only, or that OU and its child OUs.
- Managing permissions is easier and more efficient if you assign control at the highest OU level possible.
- Authority delegated at the site level is likely to span domains and can influence objects in domains other than the domain where the GPO is located.

Following are descriptions of how to use GPMC to perform these delegation tasks.

Delegating management of individual GPOs

Using GPMC, you can easily grant additional users permissions on a GPO. GPMC manages permissions at the task level. There are five levels of allowed permissions on a GPO: Read, Edit, and Edit/Delete/Modify Security, Read (from Security Filtering), and Custom. These permission levels correspond to a fixed set of low-level permissions. Table 2.4 shows the corresponding low-level permissions for each option.

Table 2.4 GPO Permission Options and Low Level Permissions

GPO Permission Option	Low Level Permissions
Read	Allow Read Access on the GPO.
Read (from Security Filtering)	This setting cannot be set directly, but appears if the user has Read and Apply Group Policy permissions to the GPO, which is set using Security Filtering on the **Scope** tab of the GPO.
Edit settings	Allow Read, Write, Create Child Objects, Delete Child Objects.
Edit, delete, and modify security	Allow Read, Write, Create Child Objects, Delete Child Objects, Delete, Modify Permissions, and Modify Owner. This essentially grants full control on the GPO, except that the "Apply Group Policy" permission is not set.
Custom	Any other combinations of rights, such denying permissions, appear as **Custom** permissions. You cannot set custom rights by clicking **Add**. They can only be set by using the ACL editor directly, which can be started by clicking the **Advanced** button.

You can click **Add** to grant users permissions on a GPO. This starts the object picker so you can find the desired user or group to set the permission level. You can then set the permission level by selecting the **Read**, **Edit**, or **Edit, Delete, Modify Security** permissions.

Note that the **Apply Group Policy** permission, which is used for Security Filtering, cannot be set using the **Delegation** tab. Because setting **Apply Group Policy** is used for scoping the GPO, this

permission is managed on the **Scope** tab of the GPMC user interface. When you grant a user Security Filtering on the **Scope** tab, you are actually setting both the **Read** and **Apply Group Policy** permissions.

You can grant additional groups and users permissions on a GPO by using GPMC, as described above. Table 2.5 lists the default security permission settings for a GPO.

Table 2.5 Default Security Permissions for GPOs.

Security Group	Permissions
Authenticated Users	Read (from Security Filtering)
Enterprise Domain Controllers	Read
Domain Administrators Enterprise Administrators	Edit settings, delete, modify security
Creator Owner	
SYSTEM	

Note

- Because Administrators are also part of the Authenticated Users group, they have the Apply Group Policy ACE set to Allow by default; as a result, policy settings apply to them as well if they are located in the container where the GPO is linked.

Delegating Group Policy-Related Tasks on Sites, Domains, and OUs

You can manage three Group Policy tasks on a per-container basis in Active Directory:

- Linking GPOs to an Active Directory container (site, domain, or OU)
- Performing Group Policy Modeling analysis for objects in that container (domains and OUs)
- Reading Group Policy Results data for objects in that container (domains and OUs)

By default, Domain Administrators have GPO linking permission for domains and OUs, and Enterprise Administrators and Domain Administrators of the forest root domain can manage links to sites. You can delegate permissions to additional groups and users by using GPMC.

By default, access to Group Policy Modeling and remote access to Group Policy Results data is restricted to Enterprise Administrators and Domain Administrators. Organizations can delegate access to these tasks to lower-level administrators by setting these permissions in GPMC.

The following procedures detail Group Policy delegation tasks on Active Directory containers.

To delegate Group Policy administrative tasks on a container

1. To delegate Group Policy-related permission on a site, domain, or OU, click the appropriate container in the GPMC console.

2. In the right pane for the site, domain, or OU, click the **Delegation** tab.

3. In the drop-down list box, select the desired permission you want to manage: **Link GPOs**, **Perform Group Policy Modeling analyses**, or **Read Group Policy Results data**. Note that GP Modeling and GP Results are not available for sites.

4. To add new groups, use the **Add** button.

5. To modify the **Applies To** setting for an existing permission, right-click the user or group in the list and then select either **This container only** or **This container and all child containers**.

6. To remove an existing group or user from having the specified permission, select the user or group from the list and click the **Remove** button. Only domain administrators have permission to do this.

7. To add or remove custom permissions, click **Advanced** at the bottom-right of the details pane and select the object whose permissions you want to change. Note that setting custom permissions is *not* recommended.

Delegating Creation of GPOs

The ability to create GPOs in a domain is a permission that is managed on a per-domain basis. By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and SYSTEM can create new Group Policy objects. If the domain administrator wants a non-administrator or non-administrative group to be able to create GPOs, that user or group can be added to the Group Policy Creator Owners security group. Alternatively, you can use the **Delegation** tab on the Group Policy Objects container in GPMC to delegate creation of GPOs. When a non-administrator who is a member of the Group Policy Creator Owners group creates a GPO, that user becomes the creator owner of the GPO and can edit the GPO and modify permissions on the GPO. However, members of the Group Policy Creator Owners group cannot link GPOs to containers unless they have been separately delegated the right to do so on a particular site, domain, or OU. Being a member of the Group Policy Creator Owners group gives

the non-administrator full control of only those GPOs that the user creates. Group Policy Creator Owner members do not have permissions for GPOs that they do not create.

Note

- When an administrator creates a GPO, the Domain Administrators group becomes the Creator Owner of the Group Policy object. By default, Domain Administrators can edit all GPOs in the domain.

The right to link GPOs is delegated separately from the right to create GPOs and the right to edit GPOs. Be sure to delegate both rights to those groups you want to be able to create and link GPOs. By default, non-Domain Admins cannot manage links, and this prevents them from being able to use GPMC to create and link a GPO. However, non-Domain Admins can create an unlinked GPO if they are members of the **Group Policy Creator Owners** group. After a non-Domain Admin creates an unlinked GPO, the Domain Admin or someone else who has been delegated permissions to link GPOs an a container can link the GPO as appropriate.

Creation of GPOs can be delegated to any group or user. There are two methods of granting a group or user this permission:

- Add the group or user to the Group Policy Creator Owners group. This was the only method available prior to GPMC.

- Explicitly grant the group or user permission to create GPOs. This method is newly available with GPMC.

You can manage this permission by using the **Delegation** tab on the Group Policy objects container for a given domain in GPMC. This tab shows the groups that have permission to create GPOs in the domain, including the Group Policy Creator Owners group. From this tab, you can modify the membership of existing groups that have this permission, or add new groups.

Because the Group Policy Creator Owners group is a domain global group, it cannot contain members from outside the domain. Being able to grant users permissions to create GPOs without using Group Policy Creator Owners facilitates delegating GPO creation to users outside the domain. Without GPMC, this task cannot be delegated to members outside the domain.

If you require that users outside the domain have the ability to create GPOs, create a new domain local group in the domain (for example, "GPCO – External"), grant that group GPO creation permissions in the domain, and then add domain global groups from external domains to that group. For users and groups in the domain, you should continue to use the Group Policy Creator Owners group to grant GPO-creation permissions.

Adding a user to the membership of Group Policy Creator Owners and granting the user GPO-creation permissions directly using the new method available in GPMC are identical in terms of permissions.

Delegating creation of WMI filters

WMI filters are a new feature in Windows Server 2003 and Windows XP. WMI filters are created in the **WMI Filters** container in GPMC. There are two levels of permission for creating WMI filters:

- **Creator Owner**: Allows the user to create new WMI filters in the domain, but does not grant permissions on WMI filters created by other users.
- **Full Control**: Allows the user to create WMI filters, and grants full control on all WMI filters in the domain, including new filters created after users are granted this permission.

To delegate these permissions, use the **Add** button on the **Delegation** tab of the **WMI Filters** pane.

An administrator can **Add**, **Remove**, and view **Properties** for WMI Filter delegations from the **Delegation** tab. Selecting **Add** prompts for a user or group before selecting the permission level (**Creator Owner** or **Full Control**) to assign to the user or group. Selecting **Remove** prompts for confirmation that the delegation should be removed. Selecting **Properties** displays the user or group properties for that object.

Delegating permissions on individual WMI filters

GPMC allows you to delegate permissions on individual WMI filters. There are two levels of permissions that can be granted to a user or group on an individual WMI filter:

- **Edit**: Allows the user or group to edit the selected WMI filter.
- **Full Control**: Allows the user or group to edit, delete, and modify security on the selected WMI filter.

These permissions are managed by using the **Delegation** tab of a WMI filter

The **Delegation** tab shows the users and groups that have permissions on the WMI filter, their permission levels, and whether the permission is inherited from a parent container. Buttons on this tab let you add users and groups to the delegation list for the WMI filter, or remove them from this list.

Note that all users have **Read** access to all WMI filters. GPMC does not allow this permission to be removed. If the **Read** permission were removed, this can cause Group Policy processing on the destination computer to fail.