



Administering Group Policy with Group Policy Management Console

By Jim Lundy

Microsoft Corporation

Published: April 2003

Abstract

In conjunction with Windows Server 2003, Microsoft has released a new Group Policy management solution that unifies management of Group Policy. Microsoft Group Policy Management Console (GPMC) provides a single solution for managing all Group Policy-related tasks. GPMC lets administrators manage Group Policy for multiple domains and sites within one or more forests, in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management. Together these advantages make Group Policy much easier to use and help you manage your enterprise more cost-effectively.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
GPMC System Requirements.....	1
Installing GPMC.....	2
Group Policy Management Console Overview	3
Managing Multiple Forests.....	5
Domain Controllers in GPMC.....	6
Domain Contents Overview.....	8
Creating and Editing GPOs	11
Scoping GPOs	12
Linking GPOs.....	12
Security Filtering.....	14
Linking WMI Filters.....	14
Group Policy Inheritance	15
Delegating Group Policy	18
Delegating Creation of GPOs.....	18
Delegating an individual GPO.....	19
Delegating Policy-Related Permissions on SOMs.....	21
Delegating Linking of GPOs.....	22
Delegating Group Policy Modeling.....	22
Delegating Group Policy Results.....	23
Delegating Creation of WMI Filters.....	24
Delegating an individual WMI Filter.....	25
Reporting on GPO Settings	27
Administrative Templates Background.....	29
Administrative Templates and GPMC.....	29
Administrative Templates and Group Policy Object Editor.....	30
GPO Details	31
Ensuring consistency of permissions on a GPO.....	32
GPO Operations	34

Backup	34
Managing Backups	36
Restore.....	37
Special Considerations for Software Installation GPOs.....	39
Considerations for Domain Rename	40
Import.....	40
Copy.....	40
Using migration tables to facilitate cross-domain import and copy operations.....	41
Which settings are impacted by Migration Tables:.....	42
Scenarios for Copy and Import.....	46
Creating a Staging Environment.....	47
WMI Filters.....	49
Searching for GPOs	52
Group Policy Modeling	55
Group Policy Results	60
Platform Dependencies.....	62
GPMC Options	63
Internet Explorer Enhanced Security Configuration Considerations	64
Scripting Group Policy-related Tasks	65
Related Links	68

Introduction

Microsoft Group Policy Management Console (GPMC) is the new tool for Group Policy management that helps administrators manage an enterprise more cost-effectively by improving manageability and increasing productivity. It consists of a new Microsoft Management Console (MMC) snap-in and a set of scriptable interfaces for managing Group Policy.

GPMC simplifies the management of Group Policy by providing a single place for managing core aspects of Group Policy. It addresses the top Group Policy deployment requirements, as requested by customers, by providing the following functionality:

- A user interface (UI) that makes Group Policy much easier to use.
- Backup/restore of Group Policy objects (GPOs).
- Import/export and copy/paste of GPOs and Windows Management Instrumentation (WMI) filters.
- Simplified management of Group Policy-related security.
- HTML reporting of GPO settings and Resultant Set of Policy (RSOP) data.
- Scripting of policy related tasks that are exposed within this tool (not scripting of settings within a GPO).

GPMC System Requirements

GPMC helps you manage both Windows 2000 and Windows Server 2003-based domains with the Active Directory® service. In either case, the computer on which GPMC runs must be running one of the following operating systems:

- Windows Server 2003.
- Windows XP Professional with Service Pack 1 (SP1) and the Microsoft .NET Framework. In addition, a post-SP1 hotfix (QFE Q326469) is required. This QFE updates your version of gpedit.dll to version 5.1.2600.1186, which is required by GPMC. This QFE is included with GPMC, and GPMC setup will prompt you to install it. However, if the language of GPMC does not match the language of your operating system, GPMC will not install the QFE, and you will need to separately obtain and install this QFE. This QFE will be included in Windows XP Service Pack 2.

Installing GPMC

Installing GPMC is a simple process that involves running a Windows Installer (.MSI) package. All necessary files are installed to the \Program Files\GPMC folder.

1. Double-click the **gpmc.msi** package, and click **Next**.
2. Accept the End User License Agreement (EULA), and click **Next**.
3. Click **Close** to complete the installation.

Upon completion of the installation, the Group Policy tab that appeared on the Property pages of sites, domains, and organizational units (OUs) in the Active Directory snap-ins is updated to provide a direct link to GPMC. The functionality that previously existed on the original Group Policy tab is no longer available since all functionality for managing Group Policy is available through GPMC.

To open the GPMC snap-in directly, use any of the following methods:

- Click **Start**, click **Run**, type **GPMC.msc**, and then click **OK**.
- Click the **Group Policy Management** shortcut in the **Administrative Tools** folder on the Start Menu or in the Control Panel.
- Create a custom MMC console - Click **Start**, click **Run**, type **MMC**, and then click **OK**. Point to **File**, click **Add/Remove Snap-in**, click **Add**, highlight **Group Policy Management**, click **Add**, click **Close**, and then click **OK**.

To repair or remove GPMC, use **Add or Remove Programs** in Control Panel. Alternatively, run the **gpmc.msi** package, select the appropriate option, and click **Finish**.

Group Policy Management Console Overview

In the past, administrators have been required to use several Microsoft tools to manage Group Policy, such as the Active Directory Users and Computers, Active Directory Sites and Services, and Resultant Set of Policy snap-ins. GPMC integrates the existing Group Policy functionality exposed in these tools into a single, unified console, along with several new capabilities.

Built-in to GPMC is support for managing multiple domains and forests, making it possible for administrators to easily manage Group Policy across an enterprise. Administrators have complete control of which forests and domains are listed in GPMC, making it possible to display only pertinent parts of an environment.

By default, the first time GPMC is started it loads the forest and domain containing the user object logged on to the computer. Administrators can then specify which forests and domains to display. When the console is closed, GPMC automatically saves the last view and will return to that view the next time the user opens that console.

The console tree on the left side of the snap-in contains GPMC's root node **Group Policy Management**. Each forest appears as a sub node of GPMC's root node, and is named after the forest root domain for that forest, pre-pended with the word "Forest." Each forest has either three or four sub nodes of its own: Domains, Sites, Group Policy Modeling, and Group Policy Results. The Group Policy Modeling node is only shown in a forest that has the Windows Server 2003 schema for Active Directory. To perform a Group Policy Modeling analysis, you must also have at least one domain controller that is running Windows Server 2003.

Figure 1 shows GPMC with two forests, Contoso.com and Tailspintoys.com, added to the console. Tailspintoys.com is a Windows 2000 forest so the Group Policy Modeling node is not available.

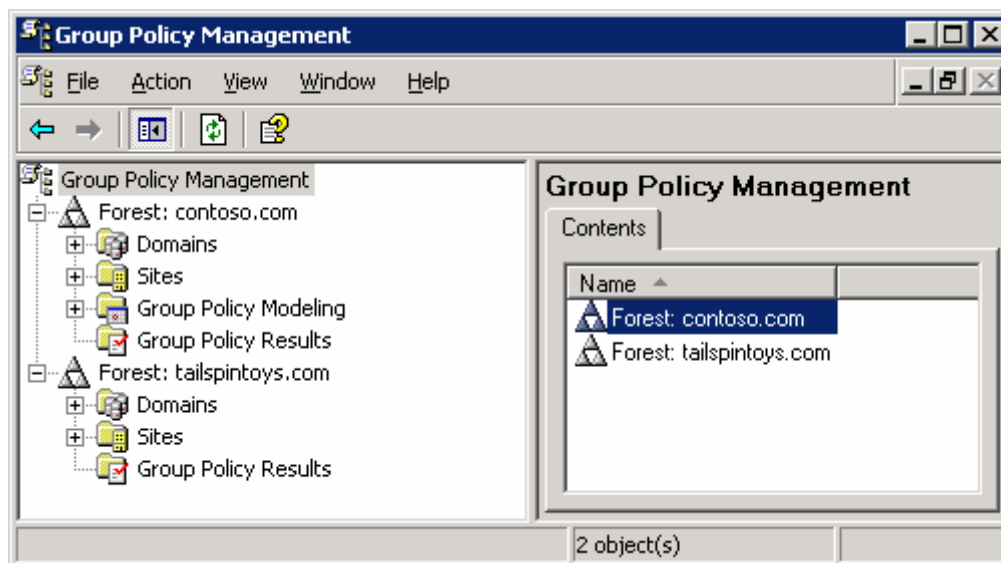


Figure 1

Below is a description of each of the four major sub node types within each forest:

- **Domains:** This node contains sub nodes corresponding to domains within the forest. The domain nodes are named after the DNS names of the domain. Users can choose which domains to display within the console, by right clicking this node and selecting the **Show Domains** context menu option. Domain nodes are always shown as peers of one another, regardless of the actual DNS relationship between them. This is because Group Policy is not inherited across domains. The list in the details pane of Figure 2 shows the name of the domain and the domain controller in that domain used during GPMC operations.

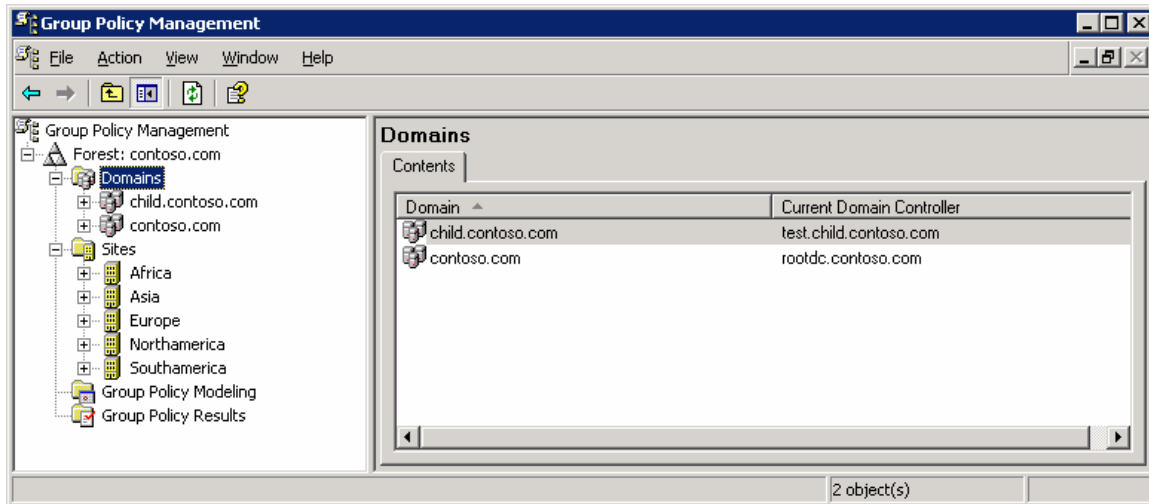


Figure 2

- **Sites:** This node contains sub nodes corresponding to sites within the forest. Users can choose which sites to display within the console, by right clicking this node and selecting the **Show Sites** context menu option. All sites are shown as peers of one another. As with forests and domains, the list of sites displayed is preserved for future use when the console is closed. No sites are displayed by default. This is done to speed up console performance by not enumerating a potentially large number of sites in the forest, unless explicitly requested by the user.
- **Group Policy Modeling:** This node allows you to access the Resultant Set of Policy (RSoP) – Planning Mode capabilities of Windows Server 2003. This is a powerful new Group Policy management feature that allows the user to simulate policy settings applied to users and computers via Group Policy before actually applying the policies. You can simulate the policy deployment for any user and computer in the forest. This feature, known as Resultant Set of Policies (RSoP) – Planning Mode in Windows Server 2003, is integrated into GPMC as Group Policy Modeling. This feature requires at least one domain controller in the forest running Windows Server 2003, since the simulation is performed by a service that is only present on domain controllers running Windows Server 2003. Each Group Policy Modeling simulation is displayed as an individual sub node.
- **Group Policy Results:** This node allows you to access the Resultant Set of Policy (RSoP) – Logging Mode capabilities. In contrast to Group Policy Modeling, which is a simulation, Group Policy Results represents the actual resultant set of policy that was applied to a given user and computer. This information is obtained by directly querying the target user/computer. Each sub node represents a different RSoP query for a given user/computer combination. You can only obtain Group Policy Results data from computers that are running Windows XP or Windows Server 2003 and later.

Managing Multiple Forests

Multiple forests can be easily added to the console tree:

1. Right-click the root node **Group Policy Management**, and select **Add Forest...**

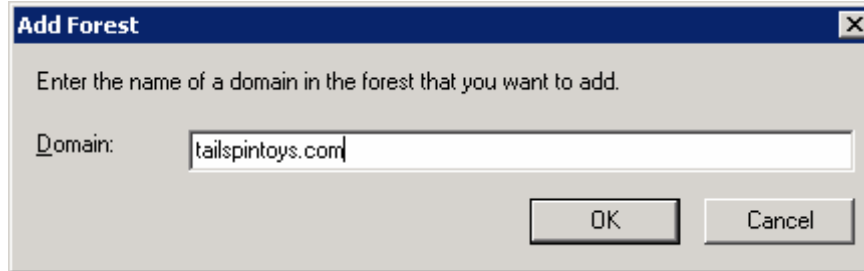


Figure 3

2. Specify the DNS or NetBIOS name of the desired domain in a forest that is not already loaded in GPMC, and click **OK**. If you specify a NetBIOS name, GPMC will attempt to determine the corresponding DNS name and will prompt you with a dialog box to confirm the entry.

The specified forest will appear as a sub node in the console tree and the forest is loaded into the console with the domain that was entered in the **Add Forest** dialog box.

To remove a forest node, simply right-click the node, and then select **Remove**.

By default you can only add a forest to GPMC if there is a 2-way trust with the forest of the user running GPMC. You can optionally enable GPMC to work with only 1 way trust or even no trust. To enable this functionality, uncheck the **Enable Trust Detection** check box on the **General** tab in the **Options** dialog box of GPMC.

If you need to add a forest to which you have no trust, you must also use the **Stored User Names and Passwords** tool to add credentials for the forest you want to connect to using the procedure below. For this procedure, assume you have no trust to a domain called "mydomain.myforest.contoso.com" and you want to manage that domain.

1. Start the **Stored User Names and Passwords** tool:
 - In Windows XP, click **Start**, click **Control Panel**, double-click **User Accounts**, click **Advanced**, and then click **Manage Passwords**.
 - In Windows Server 2003, click **Start**, click **Control Panel**, and then double-click **Stored User Names and Passwords**.
2. Add an entry for the forest containing the domain you want to manage. In this example, add the following entry:

*.myforest.contoso.com

For the user name and password, enter the name and password of an account that has the rights to access the domain you want to manage.

3. Start GPMC and disable trust detection by deselecting the **Enable Trust Detection** check box: on the **General** tab in the **Options** dialog box of GPMC.

4. Add the forest to the GPMC console by right-clicking **Group Policy Management** and then clicking **Add Forest**. Enter the name of the domain in the forest that you want to manage.

Note: When adding forests to which you have no trust, some functionality will not be available. For example, Group Policy Modeling is not available and it is not possible to open the Group Policy Object Editor on GPOs in the untrusted forest. The untrusted forest scenario is primarily intended to enable copying GPOs across forests. Microsoft will support the untrusted forest scenario on a limited basis, and will not be providing QFE or escalation support for issues arising from this scenario.

Domain Controllers in GPMC

In each domain, GPMC uses the same domain controller for all operations in that domain. This includes all operations on the GPOs, OUs, security principals, and WMI filters that reside in that domain. In addition, when the Group Policy Object Editor is opened from GPMC, it always uses the same domain controller that is targeted in GPMC for the domain where that GPO is located.

In addition, GPMC uses the same domain controller for all operations on sites. Note that this domain controller is used to read and write information about what links to GPOs exist on any given site, but information regarding the GPO itself is obtained from the domain controller of the domain hosting the GPO.

Group Policy Management Console allows you to choose which domain controller to use for each domain, as well for all sites in a forest in Group Policy Management Console. You can choose from among these four options:

- Use the primary domain controller (PDC) emulator (default choice).
- Use any available domain controller.
- Use any available domain controller that is running a Windows Server 2003 family operating system. This option is useful if you are restoring a deleted GPO that contains Group Policy software installation settings. See *Restore* for more details.
- Use a specific domain controller that you specify.

Right-click the desired domain node and select **Change Domain Controller** to specify a particular domain controller to use for domain operations.

To specify a domain controller to use for operations on sites, right click the Sites node and click **Change Domain Controller**.

In either case, the **Change Domain Controller** dialog box appears. This dialog box provides four options for specifying a domain controller as shown in Figure 4. Selecting the **This domain controller:** radio button activates the list of domain controllers allowing GPMC to target any desired domain controller in a given domain.

Note: When choosing a domain controller for sites, you have the additional option of choosing which domain to use. Using the domain dropdown list, you can efficiently filter the list of domain controllers, and select a domain controller accordingly.

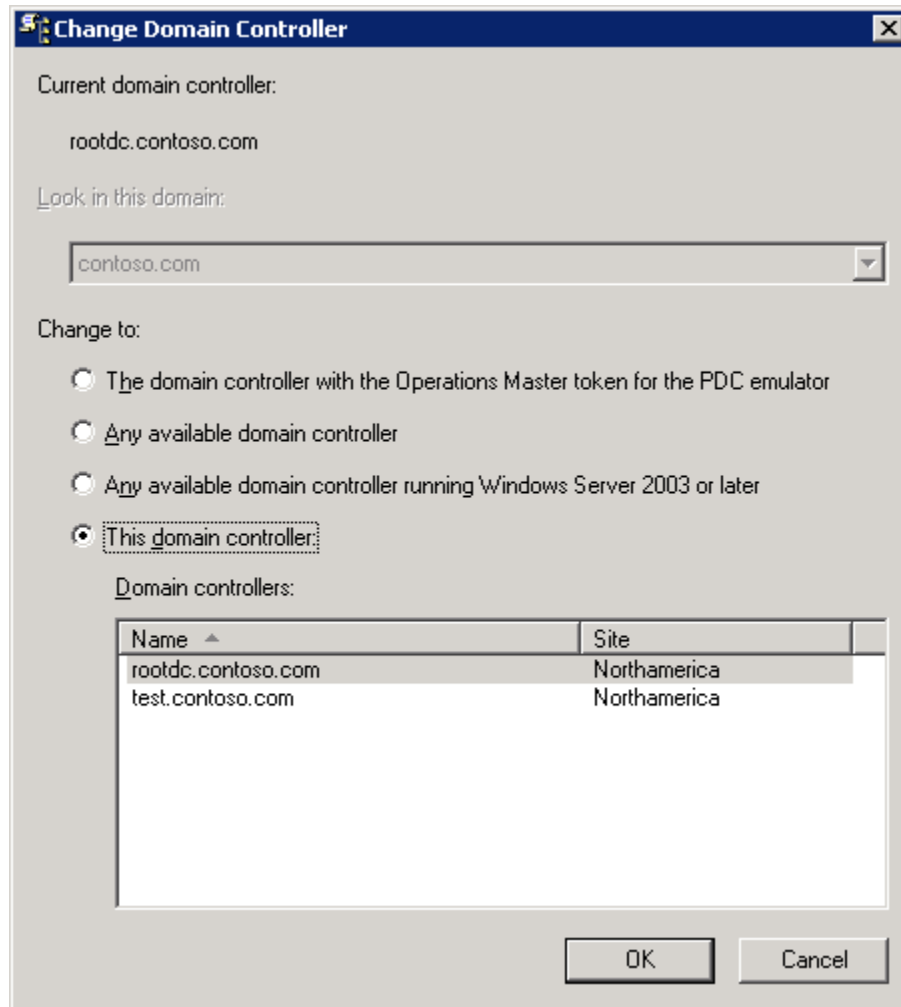


Figure 4

Selection of Domain Controllers

By default, when you add a new domain to the console, GPMC uses the PDC emulator in that domain. For managing sites, GPMC uses the PDC emulator in the user's domain by default.

It is important to consider the choice of domain controller in order to avoid replication conflicts. This is especially important to consider since GPO data resides in both Active Directory and on SYSVOL, and two independent replication mechanisms must be used to replicate GPO data to the various domain controllers in the domain. If two administrators are simultaneously editing the same GPO on different domain controllers, it is possible for the changes written by one administrator to be overwritten by another administrator, depending on replication latency.

To avoid this situation, GPMC uses the PDC emulator in each domain as the default to help ensure that all administrators are using the same domain controller. However, it may not always be desirable to use

the PDC. For example, if the administrator resides in a remote site, or if the majority of the users or computers targeted by the GPO are in a remote site, then the administrator may want to choose to target a domain controller at the remote location.

Important: If multiple administrators manage a common GPO, it is recommended that all administrators use the same domain controller when editing a particular GPO, to avoid collisions in File Replication Services (FRS).

Domain Contents Overview

Within each domain, GPMC provides a policy-based view of Active Directory and the components associated with Group Policy, such as GPOs, WMI filters, and GPO links. The view in GPMC is similar to the view in Active Directory Users and Computers MMC snap-in in that it shows the OU hierarchy. However, GPMC differs from this snap-in because instead of showing users, computers, and groups in the OUs, it displays the GPOs that are linked to each container, as well as the GPOs themselves.

Each domain node in GPMC displays the following items (see Figure 5):

- All GPOs linked to the domain.
- All top-level OUs and a tree view of nested OUs and GPOs linked to each of the OUs.
- The **Group Policy Objects** container showing all GPOs in the domain.
- The **WMI Filters** container showing all WMI Filters in the domain.

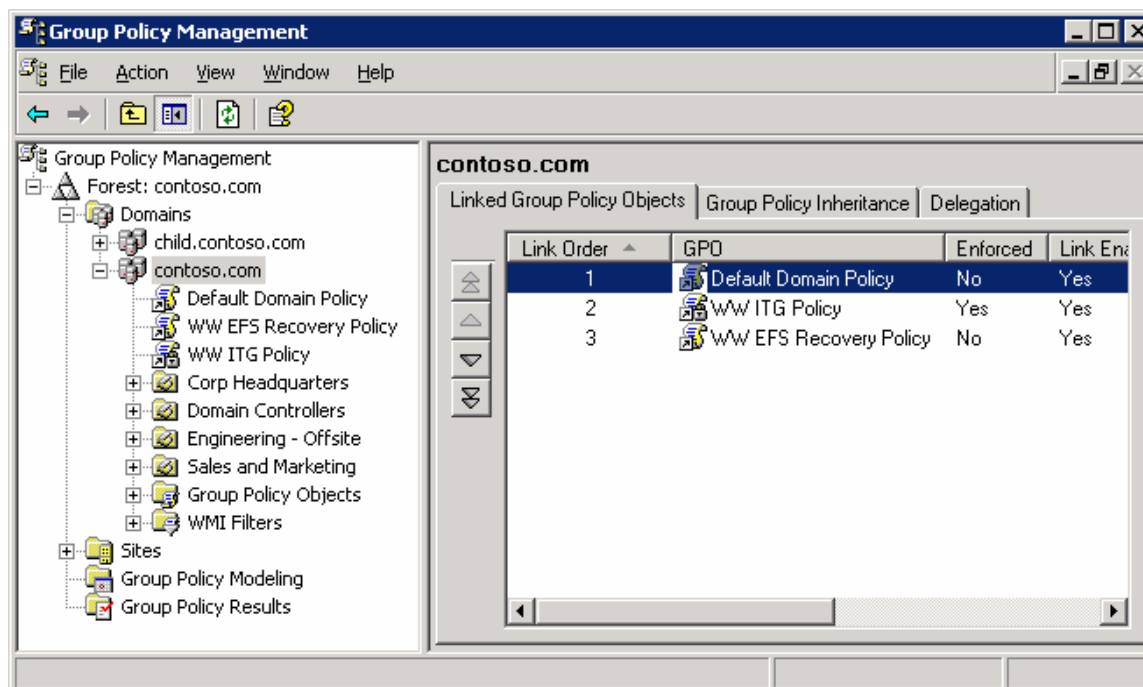


Figure 5

The **Group Policy Objects** container shows all of the GPOs for the domain. Each node in this container represents the actual GPO components from Active Directory and SYSVOL that collectively define that GPO. Figure 6 shows an expanded **Group Policy Objects** container for the Contoso.com domain containing 12 GPOs.

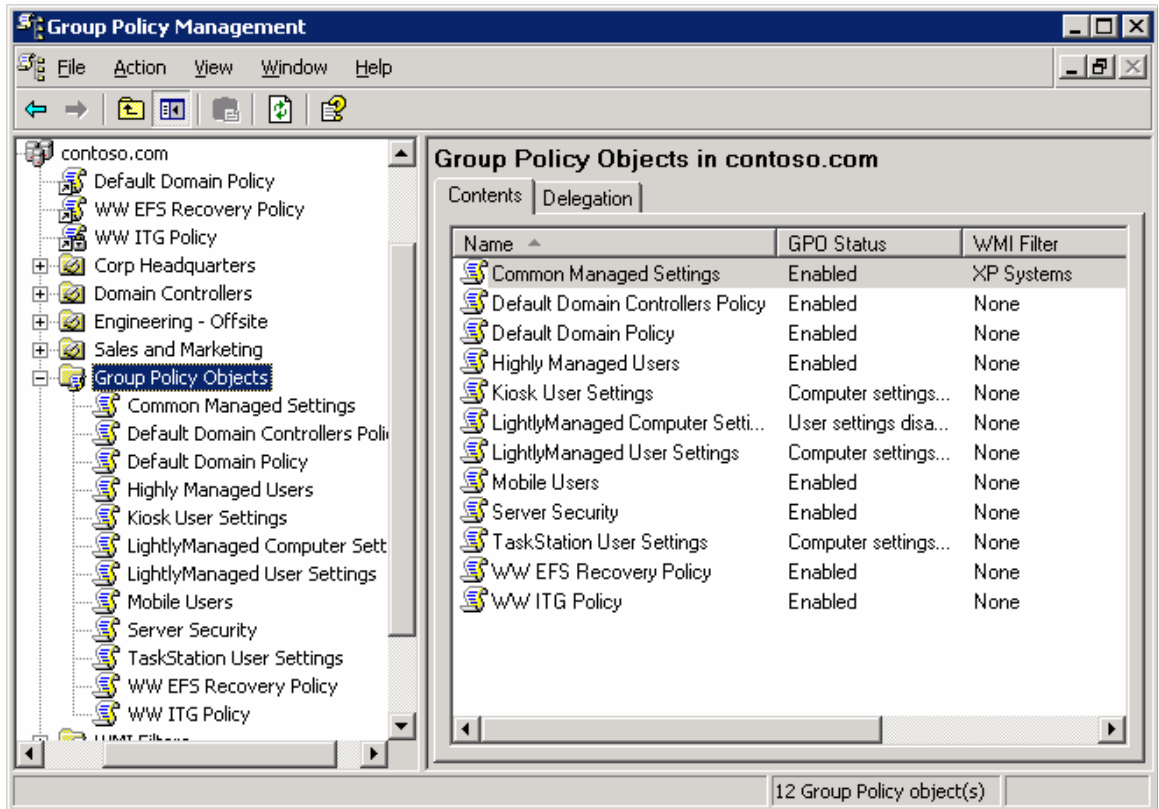


Figure 6

GPOs are not useful until they are linked to a site, domain, or OU (Scope of Management, or SOM). The settings defined in a GPO can only be applied when the GPO is linked to one or more of these SOMs. The link is not a component of the GPO; it is a component of the SOM to which it is linked. Therefore, the ability to manage links for a given SOM must be delegated on that SOM, not the GPO. In the GPMC tree view, GPO-links on a given SOM are shown as child nodes of that container.

This distinction between GPOs and GPO links was not readily apparent in Windows 2000, and a key goal for GPMC was to make this distinction clearer. The GPMC user interface distinguishes between GPO-links and GPOs as follows:

- Location in the tree view. Actual GPOs are always shown under the **Group Policy Objects** node for a given domain, whereas links appear as child nodes of a site, domain, or OU. Note that the contents of the result panes for GPOs and GPO-links are identical.
- When you click a GPO-link, a confirmation dialog box is shown by default to indicate that you are viewing a GPO-link, not a GPO.
- The icons for GPO-links have a shortcut icon, to indicate that they are pointers to another object. For example, in Figure 5, note the Default Domain Policy GPO link at the domain level. The icon for this link has a shortcut icon to differentiate it from the icon for the actual Default Domain Policy GPO under the **Group Policy Objects** node (see Figure 6).
- The context menu that appears when you right click in the tree view is different depending on whether you are managing a GPO-link or a GPO. Right clicking a GPO exposes options that are primarily relevant for the actual GPO (such as backup and restore), whereas right clicking a GPO-link exposes

options that are relevant to managing the link (such as “Enforced”). Note that some options, such as “Edit” are available on both context menus.

Creating and Editing GPOs

A Group Policy object (GPO) is a collection of policy settings that can be applied to a given set of users and/or computers. The process of applying a GPO to a set of users and/or computers is known as “scoping the GPO”, which is described later in this white paper.

With GPMC, you can create GPOs using any of the following methods:

- Right-click any domain or OU and choose **Create and Link**. This option simultaneously creates a new GPO and links that GPO to that domain or OU.
- Right-click the **Group Policy Objects** node in any domain in GPMC and click **New**. This will create a new unlinked GPO.
- Using a script. For example, GPMC includes a sample script called CreateGPO.wsf that can be run from the command line to create a new GPO.
- Using any of the methods for copying GPOs. Copy operations are described later in this white paper in the section on GPO operations.

When you create a new GPO, it initially has no settings defined. To edit the settings in a GPO, use Group Policy Object Editor (known previously as the Group Policy snap-in, Group Policy Editor, or GPedit). You can open Group Policy Object Editor by right clicking a GPO in GPMC and selecting **Edit**.

Scoping GPOs

Group Policy is a powerful tool for managing the Windows 2000 (and later) environment. The value of Group Policy can only be realized through properly applying the GPOs to the Active Directory containers you want to manage. Determining which users and computers will receive the settings in a GPO is referred to as “scoping the GPO”. Scoping a GPO is based on three factors:

- The site(s), domain(s), or organization unit(s) where the GPO is linked.
- The security filtering on the GPO.
- The WMI filter on the GPO.

This section will discuss how to utilize GPMC to properly manage the scope of a GPO and the Active Directory components you want to manage. Figure 7 shows the GPO scope tab.

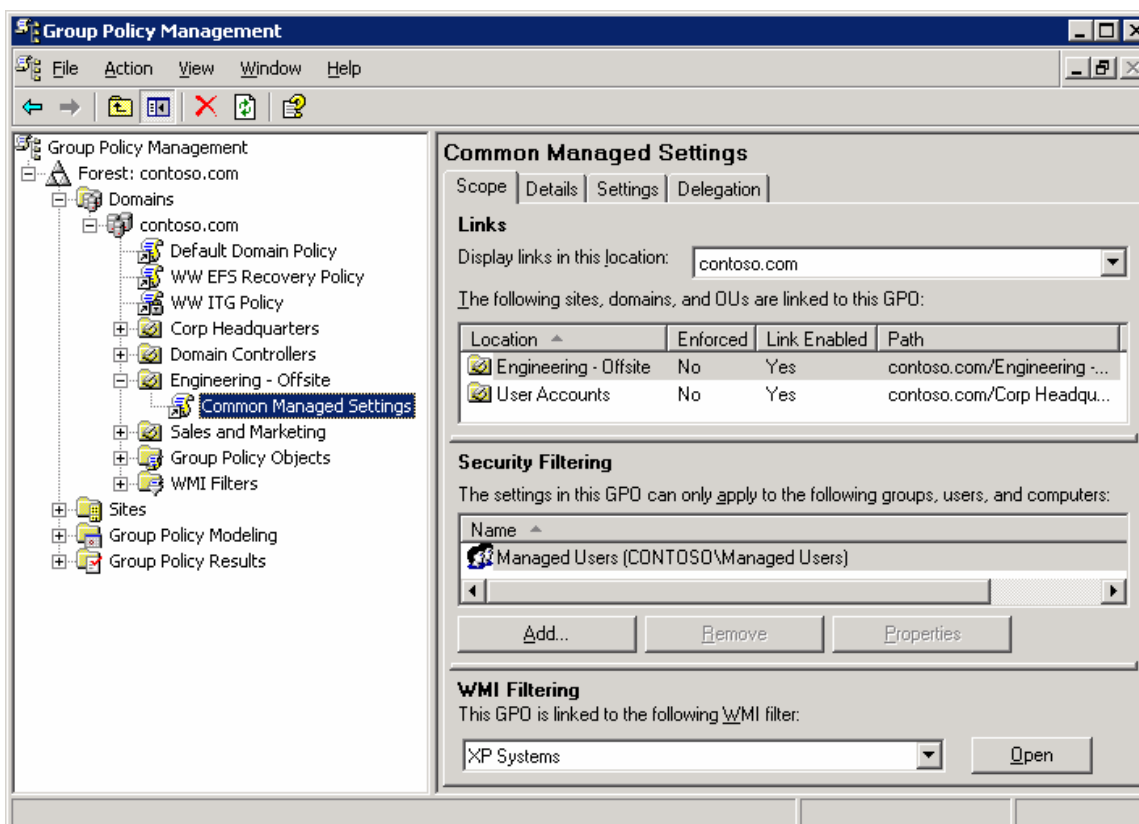


Figure 7

Linking GPOs

The primary mechanism by which the settings in a GPO are applied to users and computers is by linking the GPO to a site, domain, or OU in Active Directory. The location where a GPO is linked is referred to as the Scope of Management, or SOM (also sometime abbreviated as SDOU in previous white papers). There are three types of SOMs: sites, domains, and OUs. A GPO can be linked to

multiple SOMs, and a SOM can have multiple GPOs linked to it. A GPO must be linked to a SOM for it to be applied.

Note: GPOs are not stored on a per-SOM basis, but rather per domain. Thus, if you link a GPO to an OU, the GPO does not actually reside in that OU. A GPO is a per domain object that can be linked anywhere in the forest (although performance issues may exist where cross-domain links are used). One of the goals for GPMC is to make the distinction between links and actual GPOs clearer.

With GPMC, you can link a GPO to SOMs using any of the following methods:

- Right click a domain or OU node, and choose **Create and Link a GPO here**. This option is analogous to choosing **New** in the old Group Policy user interface prior to GPMC. (This old Group Policy interface was the Group Policy tab on the properties dialog box of a site, domain, or OU in Active Directory Users and Computers or Active Directory Sites and Services snap-ins.). Although this operation is presented as one action to the user, there are actually two operations taking place. First, a GPO is created in the domain, and second, a link to that GPO is created on the domain or OU from where you started the shortcut menu.
- Right click a site, domain, or OU node, and choose **Link an existing GPO here**. This option is analogous to choosing **Add** in the old Group Policy user interface prior to GPMC. This requires that the GPO already exists in the domain.
- Using drag and drop, drag a GPO from under the **Group Policy objects** node to the OU. This drag and drop functionality can only be performed within the same domain.

Note: By default, new user and computer accounts are created in the CN=Users and CN=Computers containers. These containers are not actually OUs, so GPOs cannot be directly applied to these containers, however, objects in these containers do inherit GPOs linked to the domain and sites.

It is possible to specify a different container in which to place either new user accounts, new computer accounts, or both. This allows you to have greater control for applying GPOs to newly created user and computer objects, before they are moved to their final locations in Active Directory. To specify new locations for user or computer accounts, use Redirusr.exe (for users) or Redircomp.exe (for computers) in the domain you want to manage. The domain administrator can use these tools to specify an OU in which to place all new user or computer accounts when they are created.

Redirusr.exe (for user accounts) and Redircomp.exe (for computer accounts) are two new tools included with Windows Server 2003 and are located in the %windir%\system32 directory.

For more information about redirecting containers for users and computers, see article Q324949, "Redirecting the Users and Computers Containers in Windows Server 2003 Domains," in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the [Web Resources page](http://www.microsoft.com/windows/reskits/webresources) at <http://www.microsoft.com/windows/reskits/webresources>.

Security Filtering

By default all Authenticated Users that are located in the SOM (and its children) where a GPO is linked will apply the settings in the GPO.

You can further refine which users and computers will receive the settings in a GPO by managing permissions on the GPO. This is known as security filtering. In order for 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, GPOs have permissions that allow the **Authenticated Users** group both of these permissions. This is how all authenticated users receive the settings of a new GPO when it is linked to a SOM (OU, domain or site). These permissions can be changed however to limit the scope of the GPO to a specific set of users, groups, and/or computers within the SOM(s) where it is linked.

GPMC simplifies how administrators manage security filtering for a GPO. Without GPMC, administrators were required to use the ACL editor, to manually set the **Read** and **Apply Group Policy** permissions for various security principals (users, computers, and groups) to modify the scope of the GPO. In GPMC, this process is no longer necessary. The administrator can just add or remove security principals in the security filtering section in the **Scope** tab for the GPO or the GPO link. This will automatically set or remove the **Read** and **Apply Group Policy** permissions for that security principal on that GPO. In the example in Figure 7, the security filtering on the “Common Managed Settings” GPO has been modified so that only members of the “Managed Users” group can receive the settings. Note that members of this group that are not located in either the “Engineering – Offsite” or “User Accounts” OUs will not receive the settings in this GPO.

If the administrator needs to access the detailed permissions, they are still available using the ACL editor when you can access using the **Advanced** button on the **Delegation** tab for the GPO. For example, if you need to set permissions to **Deny**, you can do this using the ACL editor. Groups with Deny permissions will appear as having **Custom** permissions on the **Delegation** tab. In general, it is recommended that you avoid the use of Deny permissions for managing Group Policy.

Linking WMI Filters

WMI Filters allow an administrator to dynamically determine the scope of GPOs based on attributes (available through WMI) of the target computer. A WMI filter consists of one or more queries that are evaluated to be either true or false against the WMI repository of the target computer. The WMI filter is a separate object from the GPO in the directory. To apply a WMI filter to a GPO, you link the filter to the GPO. This is shown in the WMI filtering section on the Scope tab of a GPO. Each GPO can have only one WMI filter; however the same WMI filter can be linked to multiple GPOs.

When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer. If the WMI filter evaluates to false, the GPO is not applied. If the WMI filter evaluates to true, the GPO is applied. Note that client support for WMI filters exists only on Windows XP and later operating systems. Windows 2000 clients will ignore any WMI filter and the GPO is always applied, regardless of the WMI filter.

Group Policy Inheritance

Group Policy can be applied to users and computers at a site, domain, or OU. GPOs from parent containers are inherited by default. When multiple GPOs apply to these users and computers, the settings in the GPOs are aggregated. For most policy settings, the final value of a given policy setting is set only by the highest precedent GPO that contains that setting. (However, the final value for a few settings will actually be the combination of values across GPOs.) Precedence of GPOs determined by the order of processing for the GPOs. GPOs processed last have highest precedence. GPOs follow the *SDOU* rule for processing; site first, then domain and followed by OU including nested OUs. A nested OU is one that has another OU as its parent. In the case of nested OUs, GPOs associated with parent OUs are processed prior to GPOs associated with child OUs. In this processing order, sites are applied first but have the least precedence. OUs are processed last and have the highest precedence.

There are several Group Policy options that can alter this default inheritance behavior. These options include:

- Link Order – the precedence order for GPOs linked to a given container. The GPO link with Link Order of 1 has highest precedence on that container.
- Block Inheritance – the ability to prevent an OU or domain from inheriting GPOs from any of its parent container. Note that Enforced GPO links will always be inherited.
- Enforcement – (previously known as “No Override”) the ability to specify that a GPO should take precedence over any GPOs that are linked to child containers. Enforcing a GPO link works by moving that GPO to the end of the processing order.
- Link Status – determines if a given GPO link is processed or not for the container to which it is linked.

These items are described in more detail below.

If multiple GPOs are linked to the same container and have settings in common, there must be a mechanism for reconciling the settings. This behavior is controlled by the link order. The lower the link order number, the higher the precedence. Information about the links for a given container are shown on the **Linked Group Policy Objects** tab of a given container, as in Figure 8. This pane shows if the link is enforced, if the link is enabled, the status of the GPO, if a WMI Filter is applied, when it was modified, and the domain container where it is stored. An administrator or users that have been delegated permissions to link GPOs to the container can change the link order by highlighting a GPO link and using the up and down arrows to move the link higher or lower in the link order list.

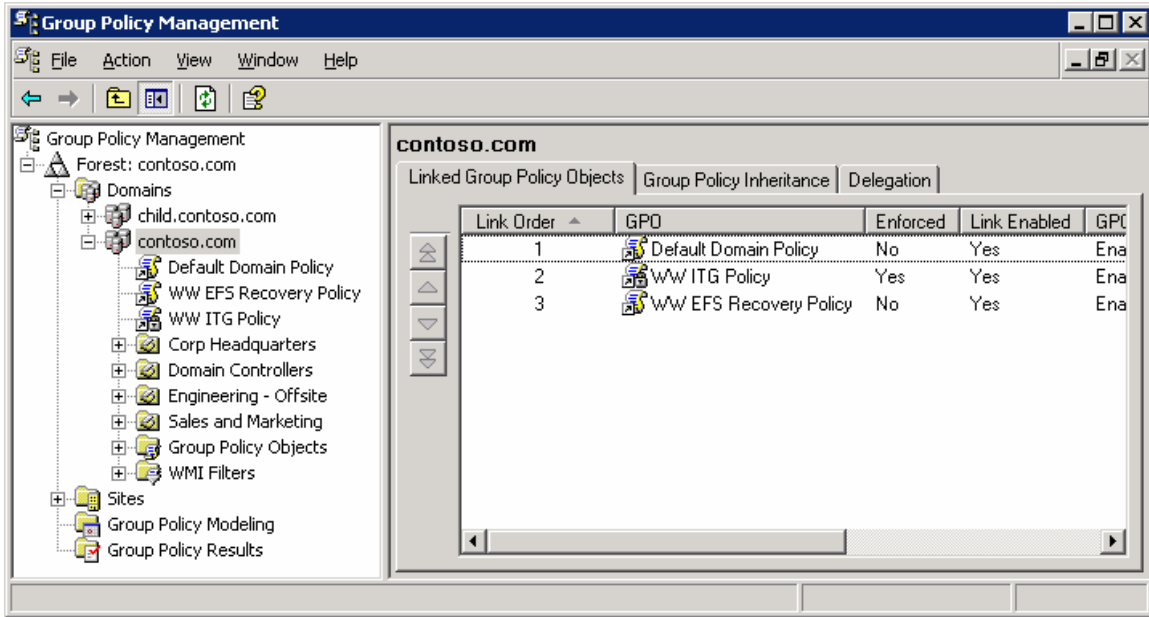


Figure 8

GPOs are inherited from parent containers. For example, a GPO linked to an OU will be inherited by child OUs. The **Group Policy Inheritance** tab for a given container shows all GPOs (except for GPOs linked to sites) that would be inherited from parent containers, as shown in Figure 9. The precedence column on this tab shows the overall precedence for all the links that would be applied to objects in that container, taking into account both Link Order and the Enforcement attribute of each link, as well as Block Inheritance on any SOMs. Note that the Group Policy Inheritance tab does NOT show the impact of GPOs linked to sites, because it is not possible to determine which site would apply, unless a particular target computer is identified.

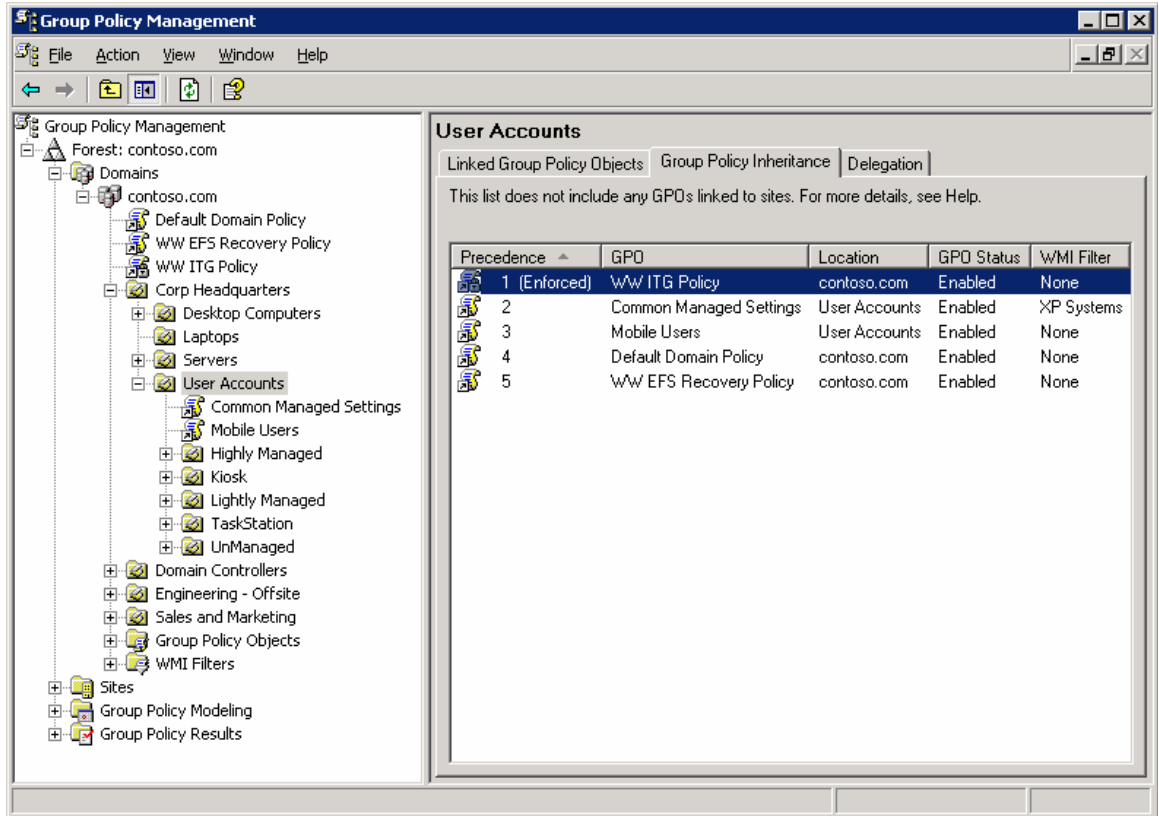


Figure 9

It is possible to prevent containers from inheriting GPOs linked to parent containers by blocking the inheritance on the OU or domain. Blocking inheritance on a container will prevent all GPOs from parent containers from applying to the blocked container, except for GPOs that are marked as Enforced. Administrators can right-click the domain or OU and select **Block Inheritance** from the context menu to set GPO blocking on the container. If inheritance is blocked for an OU or domain, its icon will appear with a blue exclamation mark in the console tree.

An administrator can prevent the settings in a GPO linked to a container from being overwritten by settings linked to GPOs in child containers (which normally would have higher precedence) by setting the GPO link to **Enforced** (formerly known as No Override). This also will prevent the GPO link from being blocked at containers that have been set to **Block Inheritance**. GPO-links that are enforced appear with a gray padlock icon in both the console tree and in the details pane.

A GPO link can be set to **Enabled** to allow it to be processed. If the link is not set to Enabled, processing of the linked GPO is disabled. The GPO link can be either enabled or disabled by right-clicking the link and selecting the **Link Enabled** option. A check beside this option indicates that the link is enabled and will be processed.

Delegating Group Policy

Group Policy is an essential component of management in Windows 2000 and Windows Server 2003 environments. A portion of Group Policy's power lies in the ability to delegate certain Group Policy tasks to other administrators. For example, the creation, linking, and editing of GPOs are independent permissions that can be delegated separately.

Group Policy delegation covers these areas:

- The ability to create GPOs in a domain.
- Permissions on an individual GPO (for example, read access, edit access).
- Permissions on an individual SOM. There are three permissions related to policy:
 - The ability to link GPOs to a SOM.
 - The ability to perform Group Policy Modeling analyses for objects in that SOM.
 - The ability to collect Group Policy Results data for objects in that SOM.
- The ability to create WMI filters in a domain.
- Permissions on an individual WMI filter (for example, edit access)

One of the key goals for GPMC was to simplify the management of Group Policy related permissions. GPMC does this by abstracting the low-level permissions on the object and managing them as a single unit, based on the task that an administrator wants to perform. Using GPMC, delegation tasks for a given object can be performed by navigating to the Delegation tab for that object.

Using this new model in GPMC, an administrator may never need the traditional ACL Editor. However, for administrators that prefer the flexibility of that ACL editor, it is still available through GPMC by clicking the Advanced button on the Delegation tab.

Delegating Creation of GPOs

Creation of GPOs is a right of the Group Policy Creator Owners (GPCO) group by default but can be delegated to any group or user. There are two methods to grant a group or user this right:

- 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 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 GPCO group. From this tab, you can modify the membership of existing groups with this permission, or add new groups.

The ability to grant users or groups permissions to create GPOs without using GPCO was added to facilitate the delegation of GPO creation to users outside the domain. Because the Group Policy

Creator Owners group is a domain global group, it cannot contain members from outside the domain. Thus, prior to GPMC, this task could not be delegated to members outside the domain.

It is recommended that for users and groups within the domain that you continue to use the GPCO group to grant them GPO creation rights. If you require that users outside the domain have the ability to create GPOs, consider using the following steps.

- Create a new domain local group in the domain (“GPCO – External” for example)
- Grant that group GPO creation rights in the domain
- Create a global group in the external domain (“GPCO in Domain X” for example)
- Add external domain groups or users to that group
- Add the global group (“GPCO in Domain X”) to the local group (“GPCO – External”)

Adding a user to the membership of GPCO, or granting the user GPO creation permissions directly using the new method available in GPMC, is identical in terms of permissions. Granting a user the ability to create GPOs in the domain does not give the user the ability to edit or delete existing GPOs or the ability to link the GPO to a SOM. Users have full control of GPOs that they created.

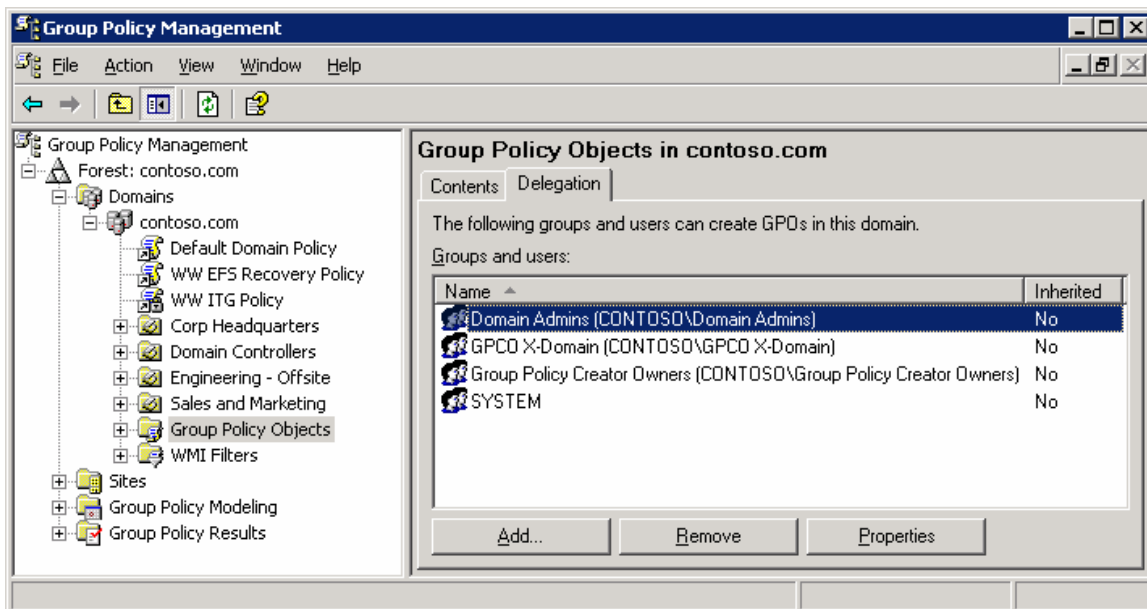


Figure 10

Figure 10 shows the results pane for the delegation tab of the Group Policy objects container in the Contoso.com domain. Domain Admins can add new delegations or remove existing delegations through the Add and Remove buttons on the delegation tab. The Properties button will display the object properties for the selected user or group.

Delegating an individual GPO

GPMC has simplified the ability to delegate rights on an individual GPO. Prior to GPMC, administrators needed to rely on the ACL editor and required an intimate knowledge of the low-level permissions on

the GPO. GPMC abstracts this so the administrator can manage the permissions on the GPO at the task level.

There are five categories of Allowed Permissions on a GPO.

- Read
- Edit settings
- Edit, delete, modify security
- Read (from Security Filtering)
- Custom

These permissions are managed using the delegation tab of a GPO, as shown in Figure 11.

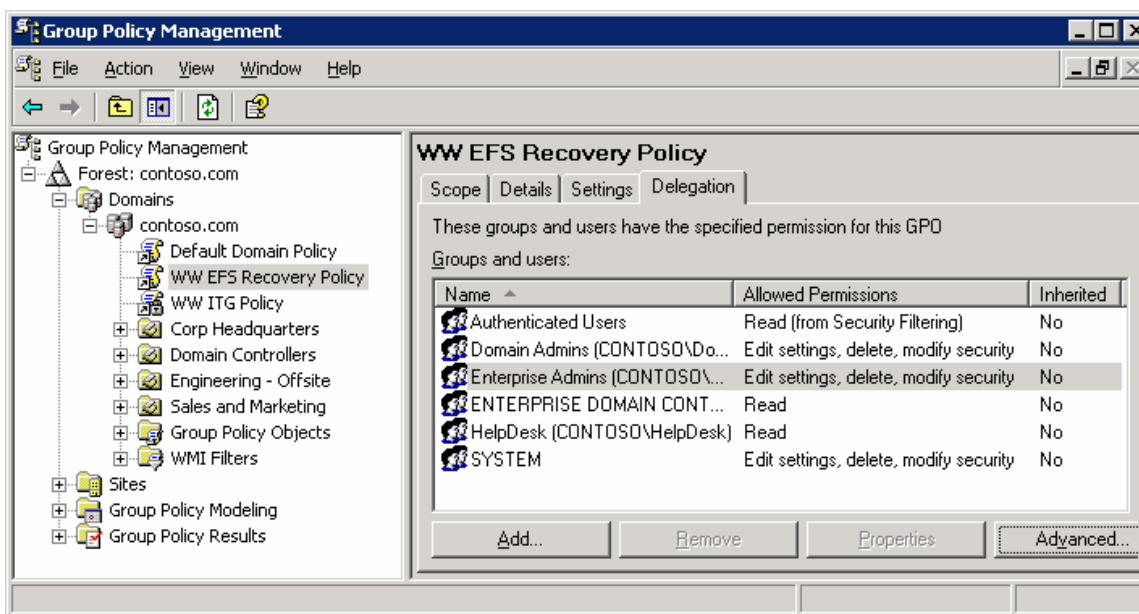


Figure 11

The options listed above represent predefined combinations of ACLs. The corresponding underlying permissions for each are shown in Table 1 below:

Table 1

Option	Underlying Permissions
Read	Allow Read Access on 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” right is not

	set.
Read (from Security Filtering)	This setting cannot be set directly, but appears if the user has Read and Apply Group Policy rights to the GPO (on the Scope tab of the GPO).
Custom	Any other combinations of rights, such as the use of deny permissions, will show up as Custom in the display. Custom rights cannot be set using the Add button, but they can be removed using the Remove button. They can be set only if using the ACL editor directly (which can be started with the Advanced button).

You can grant users permissions on a GPO using the Add button. This opens 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 either “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. Setting Apply Group Policy is used for scoping the GPO, so is managed on the Scope tab. Note that when you grant a user Security Filtering on the Scope tab, you are actually setting both the Read and Apply Group Policy rights.

Delegating Policy-Related Permissions on SOMs

GPMC enables you to easily set the following three permissions on SOMs that are related to Group Policy:

- The ability to link GPOs to a SOM.
- The ability to perform Group Policy Modeling analysis for objects in that SOM.
- The ability to collect Group Policy Results data for objects in that SOM.

These permissions are viewed and managed using the **Delegation** tab on a given SOM, and selecting the desired option from the permissions dropdown. You can add new delegations or remove existing delegations through the Add and Remove buttons on this tab. The Properties button will display the object properties for the selected user or group. The Advanced button will display the Security properties dialog box (the ACL Editor) for the SOM, from which you can view the actual permissions for the individual attributes of the SOM.

When you grant permissions using the **Add** button, you will be prompted to specify whether the permission should apply only to the current container, or whether it should be inherited to child containers. Using the **Add** button only grants “Allow” permissions. It is strongly recommended that you avoid using “Deny”. However, if you must set a “Deny” permission, you can do so by pressing **Advanced** button.

Notes:

The “Applies to” column is not present on sites as they can not have child containers.

Group Policy Modeling or Group Policy Results permissions cannot be delegated on sites so these options are not available in the permissions dropdown on site nodes.

Delegating Linking of GPOs

The settings in a GPO are applied to users and computers by linking the GPO to a SOM (site, domain, or OU) that contains the user or computer objects, either as a direct child or indirectly through inheritance. The ability to link GPOs to a SOM is a permission that is specific to that SOM. At the lowest level, the permission equates to having read and write access to the gPLink and gPOptions attributes on the SOM. However, with GPMC, there should be no need to manage these attributes individually. GPMC abstracts this permission as a single permission called “Link GPOs.” This permission also grants the ability to manage link order, block inheritance, and set the enforced attribute on GPO-links to this SOM.

This permission can be managed using the delegation tab on the SOM in GPMC when you select the **Link GPOs** option in the permission dropdown.

Figure 12 shows the **Link GPOs** permissions on the SOM delegation tab for the Child.Contoso.com domain.

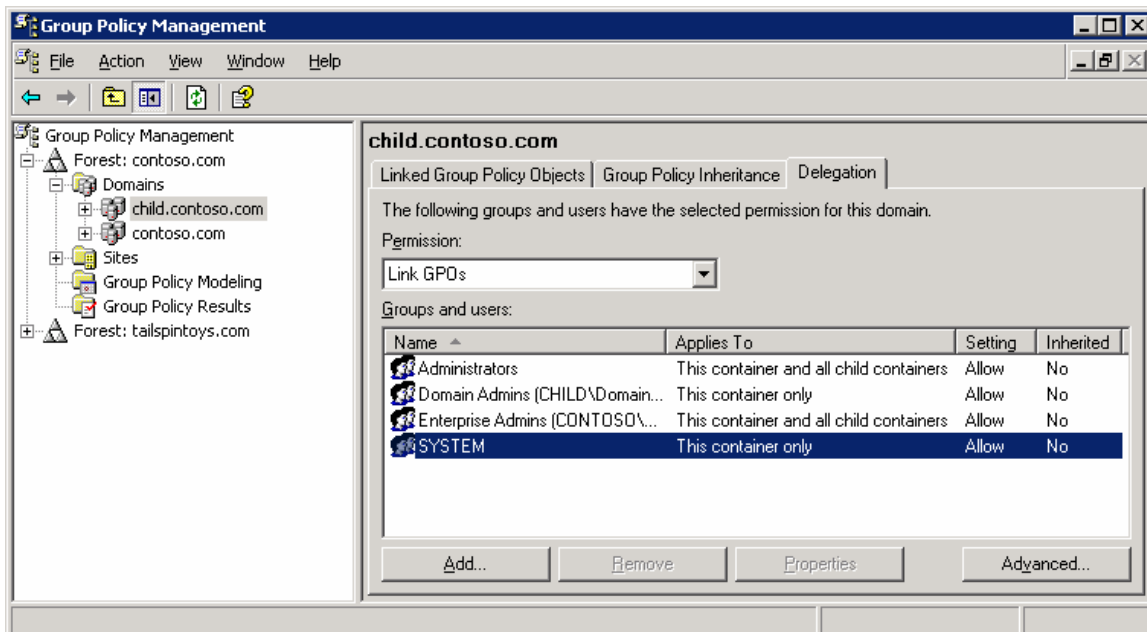


Figure 12

Delegating Group Policy Modeling

Group Policy Modeling allows the user to simulate the resultant set of policy for objects in a domain or OU. This feature is described in more detail later in the white paper. This section discusses delegation aspects only for Group Policy Modeling.

This feature is only available to Domain Administrators by default but can be delegated to other users or groups. At its lowest level, this delegation equates to granting the user or group the **“Generate Resultant Set of Policy (Planning)”** permission on an OU or domain. This permission is available in any forest that has the Windows Server 2003 schema. Without GPMC, this attribute was available only on the advanced page of the ACL editor for a given domain or OU. GPMC simplifies the management of this permission by exposing this permission directly on the **Delegation** tab for any domain or OU. The administrator selects the **“Perform Group Policy Modeling Analyses”** setting from the Permissions drop-down box. This will display the Name, Applies To, Setting, and Inherited properties for the delegations. Figure 13 shows the **Perform Group Policy Modeling Analyses** permissions on Delegation tab for the Contoso.com domain.

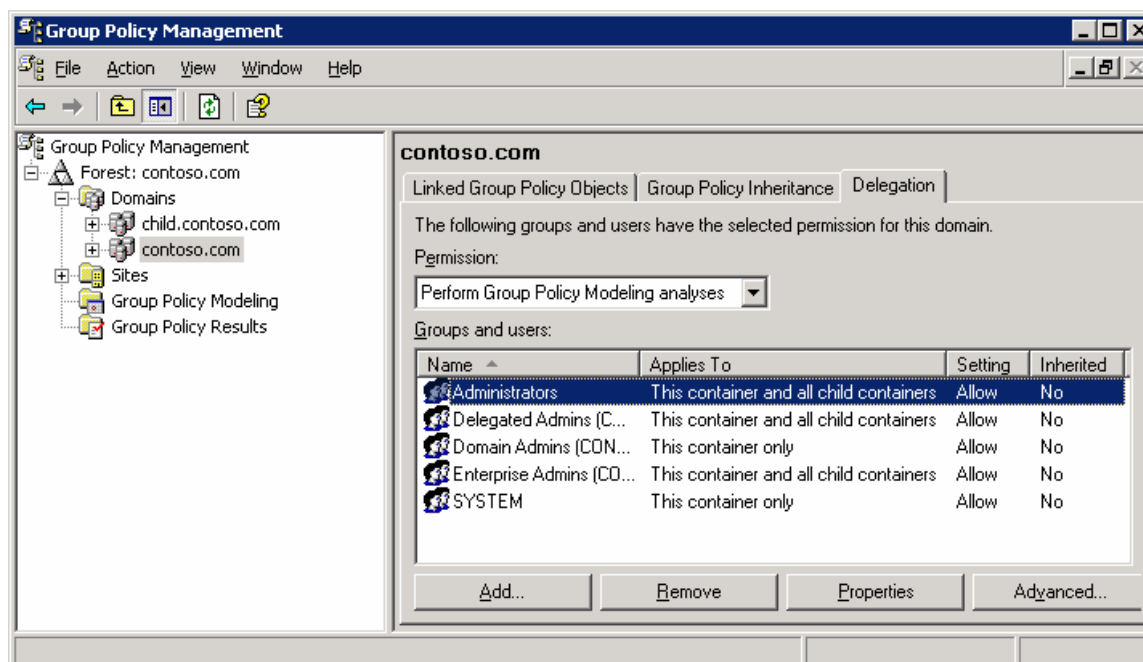


Figure 13

Delegating Group Policy Results

Group Policy Results allows the user to read RSoP logging data for objects in the domain or OU. Group Policy Results is described in more detail later in the white paper. This section discusses delegation aspects only for Group Policy Results.

By default, only users with local administrator rights on the target computer can remotely access Group Policy results data; however this right can be delegated to other users or groups. Delegation is performed on either a domain or OU. Users with this permission can read Group Policy Results data for any object in that container, and in child containers if the permission is specified to be inherited.

At its lowest level, this delegation equates to granting the user or group the **“Generate Resultant Set of Policy (Logging)”** permission on an OU or domain. This permission is available in any forest with the Windows Server 2003 schema. Without GPMC, this attribute was available only on the advanced page of the ACL editor for a given container. GPMC simplifies the management of this permission by

exposing this permission directly on the **Delegation** tab for the domain or OU. The administrator selects the “**Read Group Policy Results Data**” setting from the Permissions drop-down box. This will display the users and groups that have this permission for the domain or OU, if the setting applies to only this container or to the container and all child objects, if the setting is allowed, and if the permission is inherited from a parent container. Figure 14 shows the **Read Group Policy Results data** permissions on the Delegation tab for the Contoso.com domain.

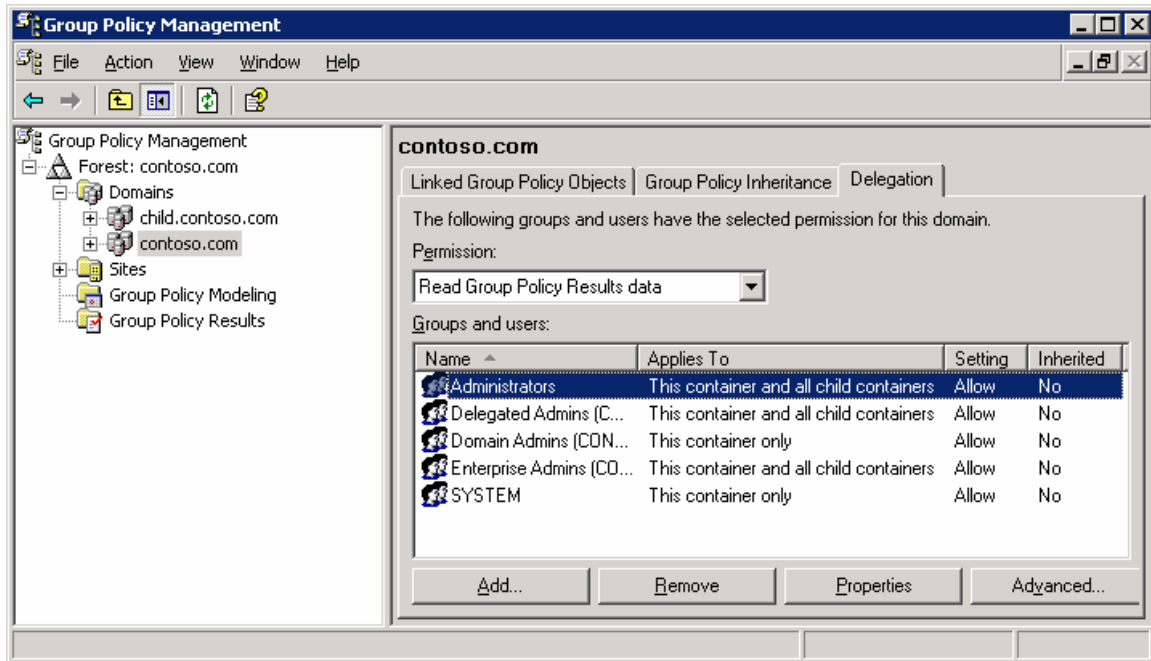


Figure 14

Delegating Creation of WMI Filters

WMI filters are a new feature in Windows Server 2003. When a new WMI filter is created it is stored in the WMIPolicy container in the domain's System container in Active Directory. It is the permissions applied on this container that govern the rights a user has to create, edit, and delete WMI Filters. This section is limited to delegation aspects of WMI filters. For more information on WMI filters, see the WMI Filters section in this white paper.

There are two levels of permission for creating WMI filters, which can only be delegated by Domain Admins:

- **Creator Owner:** Allows the user to create new WMI Filters in the domain, but does not grant them permissions on WMI filters created by other users. This permission is analogous to the GPO creation permission.
- **Full Control:** Allows the user to create WMI filters, and grants them full control on all WMI Filters in the domain, whether they created them or not. There is no corresponding permission level for GPOs because permissions in the sysvol are not inherited, so it's not technically possible to guarantee full control to all GPOs

By default, Domain Admins and Enterprise Admins have Full Control and Group Policy Creator Owners have Creator Owner permissions.

To delegate either permission to a user or group, use the Add button on the delegation tab of the WMI Filters pane. Figure 15 shows the delegation tab for the **WMI Filters** container.

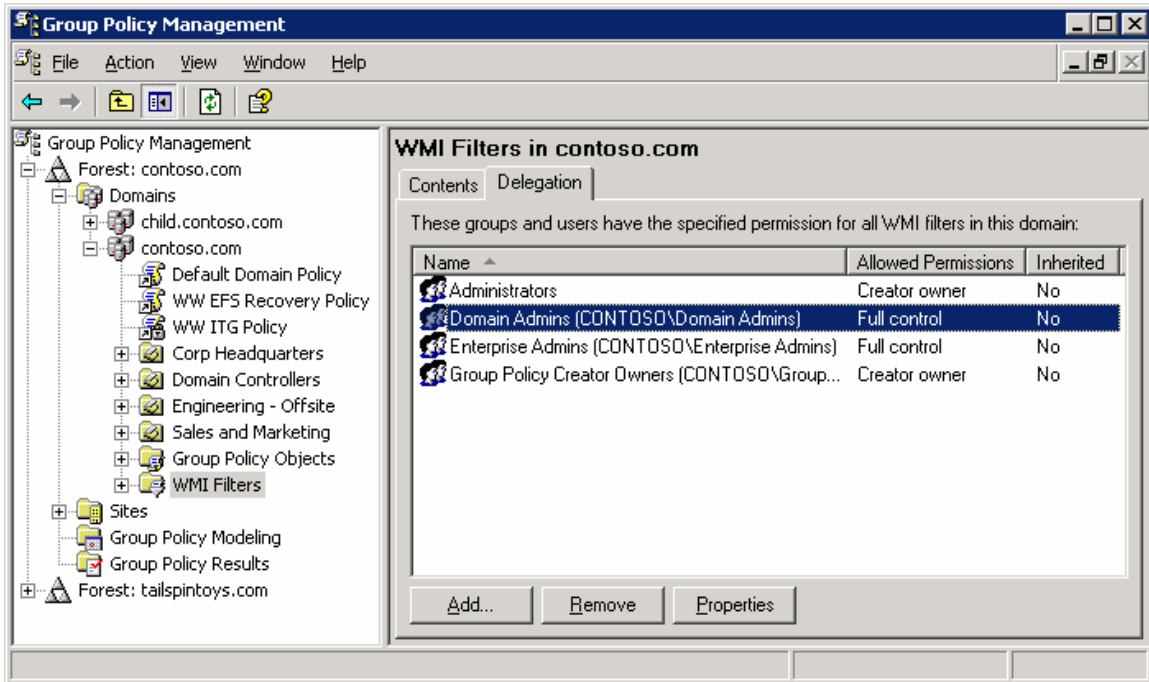


Figure 15

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

Delegating an individual WMI Filter

GPMC has the ability to delegate rights on an individual WMI Filter. 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 WMI Filter.
- Full Control – allows the user or group to edit, delete, and modify security on the WMI Filter.

These permissions are managed using the **Delegation** tab of an individual WMI Filter, as shown in Figure 16.

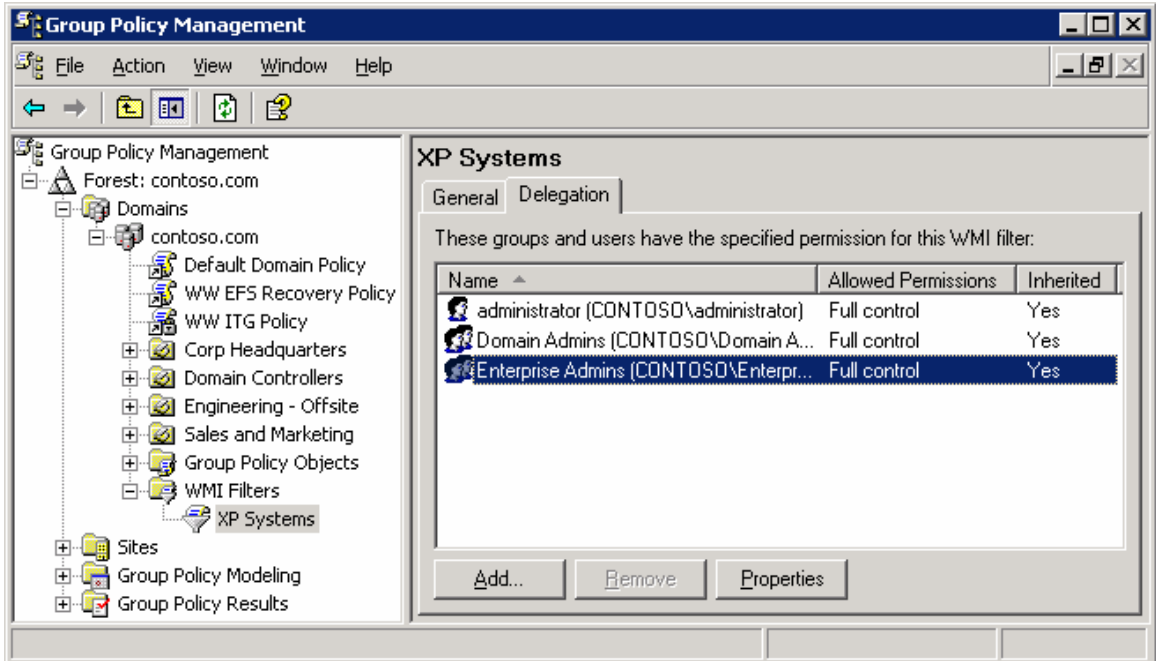


Figure 16

The **Delegation** tab shows the users and groups that have permissions on the WMI Filter, the permission level, and if the permission is inherited from a parent container. Buttons on this tab allow the user to Add or Remove users and groups to the delegation list for the WMI Filter.

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 could cause policy processing on the client to fail. Therefore, GPMC deliberately doesn't offer the capability to remove this permission.

Reporting on GPO Settings

The Settings tab of the GPO or GPO link pane in GPMC shows an HTML report that displays all the defined settings in the GPO. Clicking this tab will generate a report of the settings in the GPO. Figure 17 shows a typical report. This report can be generated by any user with read access to the GPO.

Without GPMC, users that did not have write access to a GPO could not read and view the settings in that GPO. This is because the Group Policy Object Editor requires the user to have read and write permissions to the GPO to open it. Some examples of users that might need to read and view but not edit a GPO include security audit teams that need to read but not edit GPO settings, helpdesk personnel that are troubleshooting a Group Policy issue, and OU administrators that may need to read and view the settings from inherited GPOs. With GPMC, these users now have read access to the settings.

The HTML reports also make it easy for the administrator to view all settings that are contained in a GPO at a glance. By clicking the **Show All** option at the top of the report, the report is fully expanded and all settings are shown. Alternatively, administrators can expand and contract individual sections within the report by clicking the heading for each section.

For settings under the Administrative Templates section of the report, you can view a description of the setting by clicking the setting name in the report. This opens a new window with the Explain text for that policy setting.

GPMC also solves some common reporting requirements including the ability to document all the settings in a GPO to a file for printing or viewing. Using a context menu, users can either print the reports, or save them to a file as either HTML or XML. Note that saved reports include the contents of the Settings tab, as well as additional information that is shown on the Scope, Details, and Delegation pages in the UI.

To view a saved report directly in a Web browser, you must use Internet Explorer 6 or Netscape 7. Netscape 7 does not support functionality that enables you to show or hide data in reports.

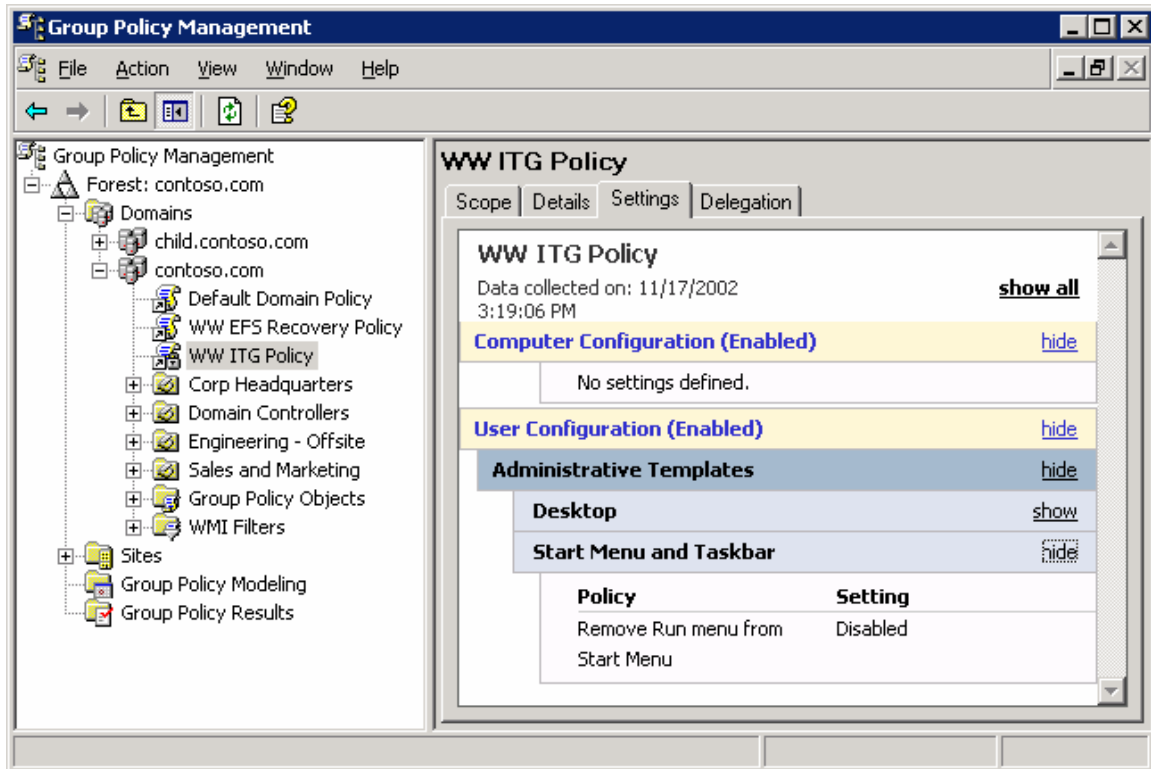


Figure 17

In addition, GPMC provides similar reports for Group Policy Modeling (Resultant Set of Policy – planning) and Group Policy Results (Resultant Set of Policy – logging). This is described later in the paper in those respective sections.

Note: The reports generated by GPMC display all settings that are contained in a GPO, except:

- Within the IE Maintenance section of reports:
 - The reports indicate only whether Content Ratings and Connectoids are deployed, and do not report the details of those settings.
 - If Preference Mode is specified, this will be indicated, however the new settings that are only available in Preference mode will not be displayed.
 - Settings for the following cookie settings which were available in IE 5.5 but not in IE 6 are not displayed:
 - Allow per-session cookies (not stored)
 - Allow cookies that are stored on your computer
 - Within Security Zones and Privacy, the details of customized Java settings, if specified, are not shown. Customized Java settings will appear as “Custom.”
 - The core information for Wireless and IPsec settings is displayed, however some details for these settings are not displayed.
-

Administrative Templates Background

Administrative templates, (or .adm files), enable administrators to control registry settings using Group Policy. Windows comes with a predefined set of Administrative template files, which are implemented as text files (with an .adm extension), that define the registry settings that can be configured in a Group Policy object (GPO). These .adm files are stored in two locations by default: inside the GPO's folder on Sysvol and in the %windir%\inf folder on the local computer.

As new versions of Windows are released, new policy settings are added. In addition to supporting these new settings, each successive version of Windows supports all registry policy settings that were available in earlier versions of Windows. For example, the Windows Server 2003 family supports all registry policy settings available in Windows 2000 and Windows XP.

It is important to understand that .adm files are not the actual settings that are deployed to client operating systems. The .adm file is simply a template file that provides the friendly name for the setting and an explanation. This template file is used to populate the user interface. The settings that are deployed to clients are contained in the registry.pol file inside the GPO. On Windows XP and Windows Server 2003, each registry setting contains a "Supported on" tag that indicates which operating system versions support that policy setting. If a setting is specified and deployed to a client operating system that does not support that setting, the settings are ignored.

Because all successive iterations of .adm files include settings from earlier versions, and because there is no harm if a new setting is applied inadvertently to a computer running an earlier operating system that does not support that setting, it is recommended to always create and edit GPOs from a computer that has the latest .adm files available.

Administrative Templates and GPMC

GPMC uses administrative templates (.adm files) to display the friendly names of policy settings in the Administrative Templates section when generating HTML reports for GPOs, Group Policy Modeling, and Group Policy Results. The reports generated by GPMC can display settings based on custom .adm files as well.

GPMC handles administrative templates for GPOs differently than the Group Policy Object Editor. The change in behavior was a deliberate design decision to simplify the behavior with .adm files, to avoid complications with .adm file version conflicts, and to improve performance in GPMC.

To generate a report, GPMC looks by default in the following locations for .adm files:

- %Windir%\inf on the local computer where GPMC is running. If an .adm file is found, it is used, regardless of its timestamp.
- If the .adm file is not found, GPMC looks in the GPO's folder on SYSVOL

The user can specify an alternate path for where to find .adm files using the custom search location option on the Reporting tab of GPMC options. If specified, this takes precedence over the previous locations.

When searching for a given .adm file, GPMC will only use the first .adm file it finds in the listed search order. If there are policy settings in the GPO for which no .adm file can be found, these settings will be displayed in the report in a section called "Extra Registry Settings" which displays the registry keys and values for those settings.

Notes:

- As noted above, GPMC looks by default on the local computer for .adm files first, since the user-specified location is not specified by default. When running GPMC on Windows XP, this means that settings that were not available in Windows XP or Windows 2000 may be displayed in the report as “Extra Registry Settings.” This situation only occurs if both of the following are true:
 - You have set one of the settings in the Administrative Templates section of the GPO that is new for Windows Server 2003.
 - You are generating a report of that GPO on a computer running Windows XP.The workaround here is to store the Windows Server 2003 versions of the .adm files somewhere, and specify that location in the custom search location mentioned above.
 - Unlike the Group Policy Object Editor, GPMC itself never transfers newer versions of .adm files to the SYSVOL. It simply reads the .adm files found using the algorithm described above in order to generate the report. However, when the Group Policy Object Editor is opened (either from GPMC or using other means) .adm files may be transferred to the sysvol, as described below.
-

Administrative Templates and Group Policy Object Editor

- The Group Policy Object Editor uses .adm files to display available policy settings in the Administrative Templates section of a GPO.
- By default it attempts to read .adm files from the GPO (from the Sysvol on the domain controller). Alternatively, the .adm file can be read from the local workstation computer. This behavior can be controlled by a policy setting.
- By default, if the version of the .adm file found on the local computer is newer (based on the time stamp of the file) than the version on the Sysvol, the local version is copied to the Sysvol and is then used to display the settings. This behavior can be controlled by a policy setting.
- If the GPO contains registry settings for which there is no corresponding .adm file, these settings cannot be seen in the Group Policy Object Editor. However, the policy settings are still active and will be applied to users or computers targeted by the GPO.

GPO Details

There are a variety of details about GPOs that are useful for troubleshooting and other purposes. For example, since the data for a given GPO is stored in both Active Directory and Sysvol, it's important to have details about of these components. As shown in Figure 18, the **Details** tab of any GPO displays this type of information and other useful attributes.

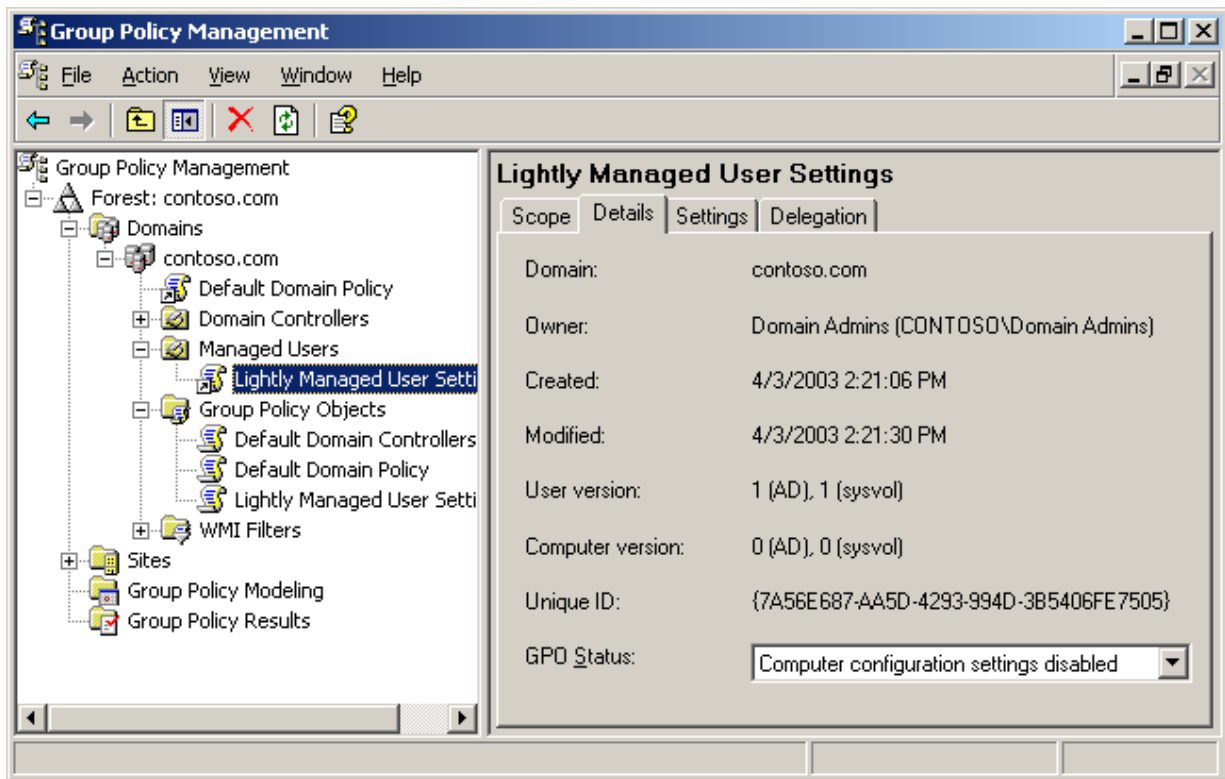


Figure 18

The **Details** tab of a GPO shows the following information:

- The domain where the GPO is defined.
- The owner of the GPO. In most cases this is the user that created the GPO. However, if a member of the Domain Admins group creates the GPO, then Domain Admins will be the owner.
- The date and time when the GPO was created.
- The date and time when the GPO was last modified.
- The version number for the user configuration component of the GPO. This is broken out into a version number for the Active Directory component and the Sysvol component. In a healthy GPO, these numbers should match. However, the user version numbers need not match the computer version numbers.

- The version number for the computer configuration component of the GPO. This is broken out into a version number for the Active Directory component and one for the Sysvol component. In a healthy GPO, these numbers should match. However, the computer version numbers need not match the user version numbers.
- The unique ID of the GPO, also known as the GPO GUID.
- The GPO Status. This indicates whether either the user configuration or computer configuration of the GPO is enabled or disabled. It can have four possible values:
 - Enabled.
 - User configuration settings disabled.
 - Computer configuration settings disabled.
 - All settings disabled.

Ensuring consistency of permissions on a GPO

Each Group Policy object (GPO) is stored partly in the Sysvol on the domain controller and partly in Active Directory. GPMC, Group Policy Object Editor, and the old Group Policy user interface provided in the Active Directory snap-ins present and manage a GPO as a single unit. For example, when you set permissions on a GPO in GPMC, GPMC is actually setting permissions on objects in both Active Directory and the Sysvol.

It is essential that the permissions in the Active Directory component are consistent with the Sysvol component for a given GPO. It is not recommended that you manipulate these separate objects independently outside of GPMC and Group Policy Object Editor. Doing so can potentially cause Group Policy processing on the client to fail, or certain users that should normally have access may no longer be able to edit a GPO. Furthermore, file system objects and directory service objects don't have the same available permissions since they are different types of objects. So in the event of a permissions mismatch, it might not be immediately apparent how to make them consistent.

To help you ensure that the security for the Active Directory and Sysvol component of a given GPO is consistent, GPMC will automatically check the consistency of the permissions of any GPO when you navigate to the GPO using GPMC. If it detects a problem with that GPO, you will be presented with one of the following dialog boxes, depending on whether you have permission to modify security on that GPO:

- “The permissions for this GPO in the SYSVOL folder are inconsistent with those in Active Directory. It is recommended that these permissions be consistent. To change the permissions in SYSVOL to those in Active Directory, click OK.”
- “The permissions for this GPO in the SYSVOL folder are inconsistent with those in Active Directory. It is recommended that these permissions be consistent. Contact an administrator who has rights to modify security on this GPO.”

If you have permission to modify security on the GPO, you should click OK in this dialog box. This action will reset the permission on the Sysvol component of the GPO to be consistent with the existing permissions on the Active Directory component of the GPO. Note that the information presented on the Delegation tab (and Security Filtering section) for a GPO is based on the Active Directory component of

the GPO, so this will simply correctly ensure that the permissions you see in the GPMC UI are being applied to that GPO.

Note: When running GPMC in a Windows 2000 domain, clicking on either the Default Domain Policy or the Default Domain Controllers Policy opens the dialog box described above. This is the result of a bug in Windows 2000 that is expected to be fixed in Windows 2000 Service Pack 4. The issue occurs because the Access Control List (ACL) on the Sysvol portion of the GPO is mistakenly set to inherit permissions from the parent folder. If you have permissions to modify security on the default GPOs, you should click OK in this dialog box. This will correct the problem by modifying the ACLs on the Sysvol portion to make them consistent with the ACLs on the Active Directory component. In this case, it will remove the inheritance attribute in the Sysvol.

GPO Operations

GPO operations refer to the ability to **backup** (export), **restore**, **import**, and **copy** GPOs.

Backing up a GPO consists of making a copy of GPO data to the file system. Note that the **Backup** function also serves as the export function for GPOs. Backed up GPOs can be used either in conjunction with Restore or Import operations.

Restoring a GPO takes an existing GPO backup and re-instantiates it back in the domain. The purpose of a restore is to reset a specific GPO back to the identical state it was in when it was backed up. Since a restore operation is specific to a particular GPO, it is based on the GUID and domain of the GPO. Therefore, a restore operation cannot be used to transfer GPOs across domains.

Importing a GPO allows you to transfer settings from a backed up GPO to an existing GPO. You can perform this operation within the same domain, across domains, or across forests. This allows for many interesting capabilities such as staging of a test GPO environment in a lab before importing into a production environment.

Restoring and Importing a GPO will remove any existing settings already in the GPO. Only the settings in the backup will be in the GPO when these operations are complete.

Copying a GPO is similar to an export/import operation only the GPO is not saved to a file system location first. In addition, a copy operation creates a new GPO as part of the operation, whereas an import uses an existing GPO as its destination. These operations are discussed in additional detail in the following sections.

Backup

Backing up a GPO places a copy of all relevant GPO data into a specified file system location. The relevant data includes:

- The GPO GUID and domain.
- GPO Settings.
- The Discretionary Access Control List (DAACL) on the GPO.
- WMI filter link (but not the filter itself).

A backup operation only backs up components of a GPO that are in the GPO in Active Directory and in the GPO file structure in SYSVOL. The operation does not capture items stored outside the GPO, such as WMI filters, links on a SOM to that GPO, and IP Security policies. These are separate objects with their own set of permissions, and it is possible that an administrator performing either a backup or restore operation may not have the required permissions on those other objects. In addition, in the case of WMI filters and IP Security policies, these can be used by multiple GPOs, so it is not necessarily desirable to restore these objects when restoring a single GPO. To avoid these complications, the backup and restore operations only handle the contents of the GPO itself.

Note that the link to a WMI filter is actually an attribute of the GPO, so the link is included as part of the GPO backup and restore operation; even though the WMI filter itself is not. Customers who want to backup and restore WMI filters should use the import and export capabilities that are available on the

WMI filter node in GPMC. Similarly, a backup operation only includes the link to any IP Security policy set in a GPO, because IPSec policies are stored outside the GPO. You must use the **Export Policies** and **Import Policies** commands of the IP Security Policy Management snap-in to back up and restore the IPSec policies themselves.

The backup also contains an XML report of the GPO settings, a date and time stamp, and the user supplied description. The report can be viewed as HTML from within GPMC. Each backup is given a unique ID. This allows for multiple GPOs and/or multiple versions of the same GPO to be backed up to the same file system location. With GPMC, users can identify backups stored in a given file system location based on GPO GUID, the GPO friendly name, the date and time stamp of the backup, the domain name, and the description of the backup. You can manage backups from within GPMC using the Manage Backups dialog box, described later in the **Managing Backups** section.

Administrators can backup one or more GPOs using the following methods:

- Right click a GPO under the **Group Policy objects** node and choose **Back up...** from the context menu.
- Right click one or more GPOs in the **Contents** tab of the **Group Policy objects** node and choose **Back up...** from the context menu. This will backup the selected GPO(s).
- On the **Group Policy Objects** node, right click and choose the **Back Up All...** option. This will backup all GPOs in the domain. This is shown in the figure below.
- Use GPO backup scripts. You can either write your own scripts, or you can use the sample scripts included with GPMC in the GPMC\scripts folder. There are two scripts **BackupGPO.wsf** and **BackupAllGPOs.wsf** that are included with GPMC that you can use to back up GPOs.

When you backup a GPO, you must supply the file system location, and optionally, a description for the backup.

Important: The administrator should take precautions to secure this location to trusted administrators only. This should be done to protect the GPO backups from malicious or accidental tampering that could compromise the environment if they were used as the basis for a restore or import operation.

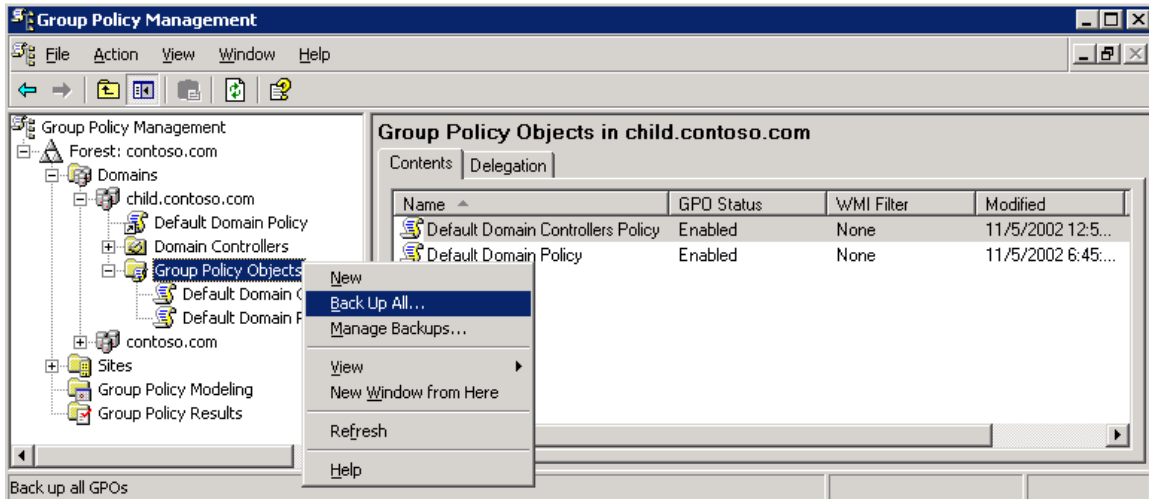


Figure 19

Backing up a GPO requires read access to the GPO and write access to the file system location where the backup will be stored.

Managing Backups

GPMC provides a way to manage the GPO backups. This feature can be accessed in 2 ways:

- Right-clicking on the **Domains** container and selecting **Manage Backups** from the context menu. This will show backed up GPOs for all domains and forests in the specified file system location.
- Right-clicking on the **Group Policy Objects** container in a domain in GPMC and selecting **Manage Backups**. This will only show GPOs backed up for that domain in the specified file system location.

Either method of starting **Manage Backups** will provide a dialog box for selecting the location of your stored GPO backups. Select a file system location containing valid GPO backups. Figure 20 shows the **Manage Backups** dialog box.

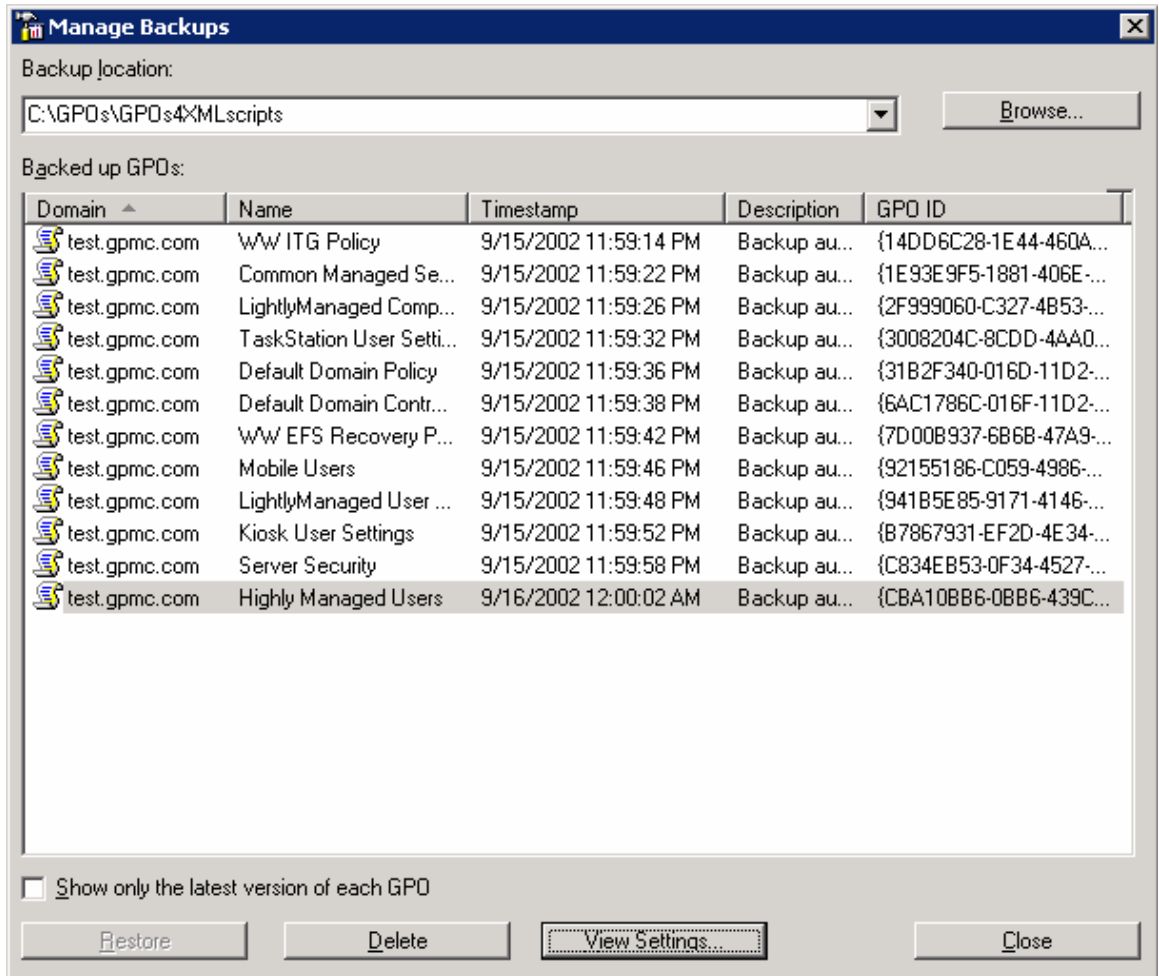


Figure 20

In the Manage Backups dialog box, you can sort, delete, restore, and view the backup settings for GPOs. Note the check box that gives the user an option to only show the latest version for each backed up GPO. The dialog box displays the originating domain for the GPO, the display name of the GPO, the timestamp when the GPO was backed up, a user supplied description when the backup was taken, and the GPO GUID.

Upon selecting either the “Restore” or “Delete” buttons, the user is presented with a confirmation dialog box before the operation is performed. Selecting the “View Settings...” button opens a new instance of the user’s default web browser which displays a report of the settings in the selected GPO. Selecting “Browse” allows the user to choose the backup location. It is possible to select multiple GPOs for deleting but not for viewing or restoring.

GPO backups can also be managed from script. The sample script QueryBackupLocation.wsf, in the GPMC\Scripts folder, will display information on backups stored in a particular file system location.

Restore

Restoring a GPO restores the GPO to a previous state. A restore operation can be used in both of the following cases: the GPO was backed up but has since been deleted, or the GPO is live and you want

to roll back to a known previous state. A restore operation retains the original GPO GUID even if the restore is recreating a deleted GPO. This is a key difference between the restore operation and the import or copy operations discussed in later sections of this white paper.

A restore operation replaces the following components of a GPO:

- GPO Settings.
- ACLs on the GPO.
- WMI filter links (but not the filters themselves).

The restore operation does **not** restore links to a SOM (Scope of Management). Any existing links will continue to be used, for example, when restoring an existing GPO to a previous state. However, if the user has deleted a GPO and all links to the GPO, the user must add these links back after restoring the GPO. To facilitate recreating these links, you can view the report in the backup to identify all links in the domain of the GPO.

You can restore GPOs using any of the following methods:

- To restore an existing GPO, right-click the GPO in the **Group Policy objects** container and select **Restore from Backup...** This opens the **Restore Group Policy Object Wizard**.
- To restore a GPO that has been deleted since it was backed up, use the **Manage Backups** dialog box (refer to Figure 20 in the Managing Backups section).
- Use GPO restore scripts. You can either write your own scripts, or you can use the sample scripts included with GPMC in the GPMC\scripts folder. There are two scripts **RestoreGPO.wsf** and **RestoreAllGPOs.wsf** that are included with GPMC that you can use to restore GPOs.

There is also an option to view the settings in the backup before restoring.

The permissions necessary to perform a restore of a GPO are different for restoring an existing GPO or if you are restoring a GPO that has been deleted since it was backed up.

Table 2

GPO State	Permissions needed
Existing GPO	The user must have Edit settings, delete, and modify security permissions on the GPO in order to restore it, as well as read access to the file system location where the backup is stored. Notice that this does NOT require GPO creation rights.
Deleted GPO	The user must have the right to create GPOs in the domain, as well as read access to the file system location where the backup is stored. The person that performs the restore will become the new creator owner for the GPO.

When restoring a GPO, GPMC will handle the GPO version number differently depending on the type of restore.

- Restore of existing GPO: The GPO version number is incremented by one over the existing version number of the live GPO. This is done to guarantee that clients will apply the GPO.
- Restore of a previously deleted GPO: The GPO version number in the GPO backup is retained in the restored GPO.

Special Considerations for Software Installation GPOs

When restoring a deleted GPO that contains Software Installation settings, some side effects are possible depending on the circumstances under which the GPO is restored. This section describes those side effects and how you can avoid them.

When restoring a GPO that has been deleted, it is possible that:

- Cross-GPO upgrade relationships that upgrade applications in the GPO being restored, if any, are not preserved after restore. A cross-GPO upgrade is one where the administrator has specified that an application should upgrade another application, and the two applications are not deployed in the same GPO. Note that cross-GPO upgrade relationships are preserved when applications—in the GPO being restored—upgrade applications in other GPOs.
- If the client has not yet seen that the GPO has been deleted (either because the user has not re-logged on or rebooted since the deletion of the GPO), and the application was deployed with the option to “Uninstall this application when it fall out of scope of management,” then the next time the client logs on:
 - Published apps that the user has previously installed will be removed.
 - Assigned applications will be uninstalled before re-installation.

This behavior occurs because when the GPO is restored, the object in Active Directory that represents the application (the "deployment object") is assigned a new GUID. Because the GUID is different than the GUID of the original deployment object, Windows interprets this as a different application.

The solution is to restore the GPO using the original GUID for the deployment object. However, because the GUID is controlled by Active Directory, the only way to re-use the original GUID is to re-animate the tombstone of the deleted deployment object. Tombstone re-animation is a new feature of Windows Server 2003.

GPMC automatically attempts to re-animate these objects when performing a restore. Re-animation will succeed if each of the following is true:

- GPMC is targeting a domain controller that is running Windows Server 2003.
- The user performing the restoration has permissions to re-animate objects in the domain. By default, only Domain Admins and Enterprise Admins have this permission. You can delegate this right to additional users at the domain level using the ACL editor.
- The time elapsed between deletion and restoration of the GPO does not exceed the tombstone lifetime specified in Active Directory.

If re-animation fails, a new deployment object will be created and the previously mentioned side effects will occur.

Therefore, as a general rule, if you deploy software using Group Policy, it is recommended that you perform the restoration of GPOs that contain application deployments using a domain controller running Windows Server 2003 and that you grant the tombstone re-animation right to the users who will be performing restoration of those GPOs.

Considerations for Domain Rename

GPO Backups taken prior to a domain rename operation cannot be restored after a renaming a domain. If you are renaming a domain, be sure to backup your GPOs as soon as you complete the rename procedure. For more details on domain rename, see the documentation on Domain Rename at <http://www.microsoft.com/windowsserver2003/downloads/domainrename.msp>.

Import

The Import operation transfers settings into an existing GPO in Active Directory using a backed up GPO in the file system location as its source. Import operations can be used to transfer settings across GPOs within the same domain, cross-domain in the same forest, or cross-domain in a separate forest (also known as cross-forest).

Import operations are ideally suited for migrating Group Policy across environments where there is no trust. For example, if you have separate test and production forests with no trust, you can use import operations to migrate GPOs that you develop and verify in the test forest to the production environment. You need to be able to access a file system location from the production environment where the backed up GPOs are stored. Depending on the settings in the GPO, you may also want to use a migration table (described later in this paper) to effectively transfer the settings.

The target of an import operation is an existing GPO. The target GPO's ACLs, links to any SOMs, and link to a WMI filter are not modified during an Import operation. Importing a GPO requires edit permissions on the target GPO.

Import operations can be performed using either of the following methods:

- Right click a GPO under the Group Policy Objects node and click Import Settings. This starts a wizard that guides you through the process of selecting a backup and optionally specifying a migration table if appropriate.
- Using either the **ImportGPO.wsf** or **ImportAllGPOs.wsf** scripts that are included with GPMC.

Copy

A copy operation transfers settings using an existing GPO in Active Directory as the source and creates a new GPO as its destination. A copy operation can be used to transfer settings to a new GPO either in the same domain, cross-domain in the same forest, or cross-domain in a separate forest. Since a copy operation uses an existing GPO in Active Directory as its source, trust is required between the source and destination domains, or you must use the **Stored User Names and Passwords** tool as described earlier in the section "Managing Multiple Forests," to gain access to the untrusted forest. Copy

operations are ideally suited for migrating GPOs between production environments, as well as for migrating Group Policy that has been staged and tested in a test domain or forest to a production environment.

Copying a GPO requires GPO creation rights in the target domain and read access to the source GPO.

When copying a GPO, the administrator has two options for specifying the DACL to use on the destination GPO:

- Use the default permissions that are used when creating new GPOs.
- Preserve the DACL from the source GPO. Note that if a migration table (described in the next section) is specified during the copy operation, the migration table will apply to any security principals in the DACL.

There are some minor differences between same-domain and cross-domain copy operations.

- When copying a GPO within the same domain, any link to a WMI filter is preserved. However, when copying a GPO to a new domain, the link is dropped because WMI filters can only be linked to GPOs within the same domain.
- When copying a GPO within the same domain, any link to an IPsec policy is preserved. However, when copying a GPO to a new domain, the link is dropped because it is unknown whether a corresponding IPsec policy exists in the new domain, and it is not always desirable to link to the original IPsec policy in the original domain.
- When copying a GPO within the same domain, the user is presented with a simple choice of choosing the DACL. However, for cross-domain copy operations, GPMC presents a wizard to facilitate the operation. In the cross-domain case, the user has the ability to specify a migration table (described below).

Copy operations can be performed using any of the following methods:

- Right-click the source GPO and choose copy, and then right-click the **Group Policy Objects** container in the desired destination domain and choose the paste option.
- Using drag and drop to drag the source GPO to the **Group Policy Objects** container in the destination domain.
- Using the **CopyGPO.wsf** command-line script that is included with GPMC.

Using migration tables to facilitate cross-domain import and copy operations

This section discusses the use of migration tables to facilitate cross-domain import and copy operations.

The key challenge when migrating GPOs from one domain to another is that some information in the GPO is actually specific to the current domain where the GPO is defined. When transferring the GPO to a new domain, it may not always be desirable, or even possible, to use the exact same settings. Items that can be specific to a domain include references to security principals (users, groups, and computers) and UNC paths. The solution is to modify these references in the GPO that are domain-specific, during the import or copy operation, so that the settings in the destination GPO are written with

the appropriate information for the destination domain. GPMC supports this capability using migration tables.

A migration table is a file that maps references to users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO. The migration table consists of one or more mapping entries. Each mapping entry consists of a source type, source reference, and destination reference. If you specify a migration table when performing an import or copy, each reference to the source entry will be replaced with the destination entry when writing the settings into the destination GPO. Note to use a migration table, the security principals specified in the destination entries of the migration table must already exist when you perform the import or copy operation.

The migration table will apply to any references in the settings within a GPO, whether you are performing an import or copy operation. In addition, during a copy operation, if you choose the option to preserve the ACL on the GPO, the migration table will also apply to both the ACL on the GPO and the ACLs on any software installation settings in the GPO.

Migration tables have their own file name extension, .migtable. The mapping information is stored as XML. You can create and edit migration tables using the Migration Table Editor (MTE) described later in this section. A sample migration table file is included with GPMC installation at “%ProgramFiles%\GPMC\Scripts” as SampleMigrationTable.migtable.

Which settings are impacted by Migration Tables:

There are two types of settings that may not transfer well across domains:

1. Users, groups, and computers (security principals) that are referenced in the settings of the GPO, and optionally for copy operations, in the DACL for the GPO itself and the DACL for any software installation settings in the GPO. Security principals don't transfer well for several reasons:
 - Domain local groups are never valid in external domains.
 - If there is no trust between source and destination domains, then none of the security principals in the source domain will be available in the destination domain.
 - Even in situations with trust between source and destination domains, it may not always be appropriate to use the exact same group in the new domain.
2. UNC paths. When you are migrating GPOs from test to production, users in the production environment may not have access to paths in the test environment, and vice versa.

The following items can contain security principals and can be modified using a migration table:

- Security policy settings of the following types:
 - User rights assignment
 - Restricted groups
 - System services
 - File system
 - Registry
- Advanced folder redirection policy settings.

- The GPO DACL, if you choose to preserve it during a copy operation.
- The DACL on software installation objects – only preserved if the option to copy the GPO DACL is specified.

The following items can contain UNC paths, which can be updated to new values as part of the migration process:

- Folder redirection policy settings.
- Software installation policy settings (for software distribution points).
- Pointers to scripts deployed through Group Policy (startup, shutdown, logon, and logoff) that are stored outside the GPO. Note that the script itself is not copied as part of the GPO copy operation, unless the script is stored inside the source GPO.

Note that security principals and UNC paths referenced in other types of settings not mentioned above, such as Administrative Templates and Software Restriction Policies, cannot be mapped using migration tables.

Options for specifying migration tables

Migration tables are specified when performing import and copy operations. There are three options for using migration tables with import and copy:

- Do not use a migration table. This option will copy all references in the source GPO exactly as is.
- Use a migration table. This option will map any references in the GPO that are in the migration table. References in the source GPO that are not contained in the migration table will be copied as is.
- Use a migration table exclusively. This option requires that all references to security principals and UNC paths be specified in the migration table. If a security principal or UNC path is referenced in the source GPO and is not included in the migration table, the import or copy operation will not proceed. This option is useful to ensure you have accounted for all security principals and UNC paths in your migration table.

In addition, cross-domain copy operations will apply the migration table to the DACL on the GPO (and any software installation settings) if you choose the option to “Preserve or migrate the existing permissions” and you specify a migration table.

When performing a copy or import, the wizard will scan the source GPO or backup to determine if there are any references to security principals or UNC paths in the GPO. If there are, you will have the opportunity to specify an existing migration table or to create a new migration table. Note that during cross-domain copy operations, if you specify the option to “Preserve or migrate the permissions on the GPO”, the wizard will always present the opportunity to specify a migration table, since a DACL by definition contains security principals.

Creating Migration Tables

The Migration Table Editor (MTE) in GPMC allows the user to create and edit migration tables. You can open the MTE using any of the following methods:

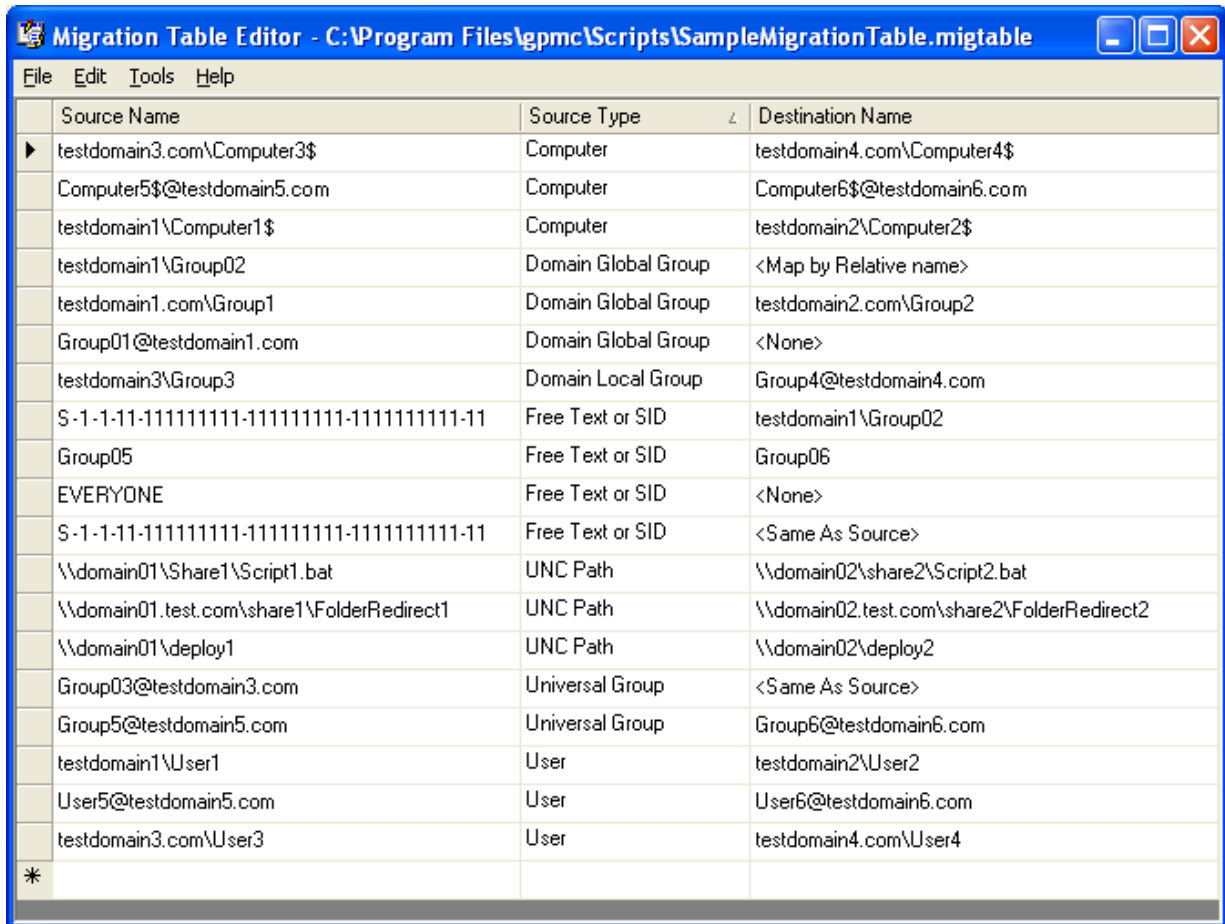
- From either the Import Settings or Cross Domain Copying wizards

- By right clicking the **Group Policy Objects** node in any domain and choosing **Open Migration Table Editor**.
- From the **Domains** node in any forest and choosing **Open Migration Table Editor**.
- By double clicking an existing .migtable file in Explorer.
- By manually running the program at %programfiles%\gpmc\mteedit.exe.

A migration table consists of one or more mapping entries, as shown in Figure 21 below. Each mapping entry has three pieces of information: Source type, source name, and destination name.

- **Source Type:** The type of domain-specific information in the domain for the source GPO. Migration tables support the following types:
 - User
 - Computer
 - Domain Local Group
 - Domain Global Group
 - Universal Group
 - UNC Path
 - Free Text or security identifier (SID). Note: This category is only for use with security principals that are specified as free text and raw SIDs.
- **Source Name:** The exact name of the User, Computer, Group or UNC Path referenced in the source GPO. The type of the source name in the source GPO or backup must match the source type specified in the migration table. Security principals can be specified using any of the following formats:
 - UPN. For example, "someone@example.com".
 - SAM. For example, "example\someone".
 - DNS. For example, "example.com\someone".
 - Free text. For example, "someone". You must specify the type as Free Text or SID in this case.
 - SID. For example, S-1-11-111111111-111111111-111111111-1112. You must specify the type as Free Text or SID in this case.
- **Destination Name:** The destination name specifies how the name of the User, Computer, Group or UNC Path in the source GPO should be treated upon transfer to the destination GPO. There are four choices:
 - *Same as source.* Copy without changes. Equivalent to not putting the source value in the migration table at all. If specified, the destination entry will appear as <Same As Source> in the MTE.
 - *None.* Removes the User, Computer or Group from the GPO. If specified, the destination entry will appear as <None> in the MTE. This option cannot be used with UNC paths.

- *Map by relative name.* For example, map SourceDomain\Group1 to TargetDomain\Group1. If specified, the destination entry will appear as <Map by Relative name> in the MTE. This option cannot be used with UNC paths.
- *Explicitly specify value.* In the destination GPO, replace the source value with the exact literal value specified in the migration table. The same format for destination entries is supported as for source names, except that raw SIDs cannot be specified.



Source Name	Source Type	Destination Name
testdomain3.com\Computer3\$	Computer	testdomain4.com\Computer4\$
Computer5\$@testdomain5.com	Computer	Computer6\$@testdomain6.com
testdomain1\Computer1\$	Computer	testdomain2\Computer2\$
testdomain1\Group02	Domain Global Group	<Map by Relative name>
testdomain1.com\Group1	Domain Global Group	testdomain2.com\Group2
Group01@testdomain1.com	Domain Global Group	<None>
testdomain3\Group3	Domain Local Group	Group4@testdomain4.com
S-1-1-11-11111111-11111111-11111111-11	Free Text or SID	testdomain1\Group02
Group05	Free Text or SID	Group06
EVERYONE	Free Text or SID	<None>
S-1-1-11-11111111-11111111-11111111-11	Free Text or SID	<Same As Source>
\\domain01\Share1\Script1.bat	UNC Path	\\domain02\share2\Script2.bat
\\domain01.test.com\share1\FolderRedirect1	UNC Path	\\domain02.test.com\share2\FolderRedirect2
\\domain01\deploy1	UNC Path	\\domain02\deploy2
Group03@testdomain3.com	Universal Group	<Same As Source>
Group5@testdomain5.com	Universal Group	Group6@testdomain6.com
testdomain1\User1	User	testdomain2\User2
User5@testdomain5.com	User	User6@testdomain6.com
testdomain3.com\User3	User	testdomain4.com\User4
*		

Figure 21

To add entries in the migration table using MTE, you can either manually type in the appropriate information or you can scan an existing GPO or GPO backup to auto-populate existing security and UNC paths in the source column. When using the auto-population methods, the destination will be set to <Same as Source> by default. The user must then adjust the destination entries in the MTE.

GPMC users can also create migration table files using the **CreateMigrationTable.wsf** script included with GPMC. This script performs an auto-populate operation that is available in the MTE. The user must then edit the file manually to set the target ACLs and paths. Alternatively, you can create a migration table manually using any XML editor.

Scenarios for Copy and Import

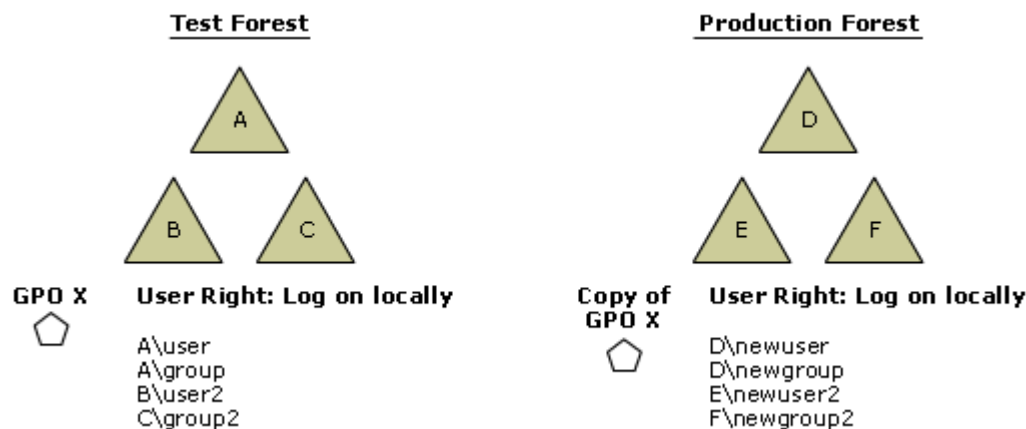
There are two key scenarios GPMC enables with the copy and import operations .

- Test-to-production migration.
- Production-to-production migration.

Test-to-production migration

The test-to-production scenario is usually a multi-forest environment with separate forests for test and production which are often physically isolated. In this scenario, all groups, users, and computers in all domains will likely need to be mapped.

Sometimes there is a trust between the forests while other times there is not. GPMC handles either scenario, and typically a migration table will be required. In cases with no trust, all security principals and UNC paths must be mapped using a migration table. Also, if there is no trust, you must either use import, or if using copy, you must supply alternate credentials using the **Stored User Names and Passwords** tool as described earlier in the section “Managing Multiple Forests,” to gain access to the untrusted forest.



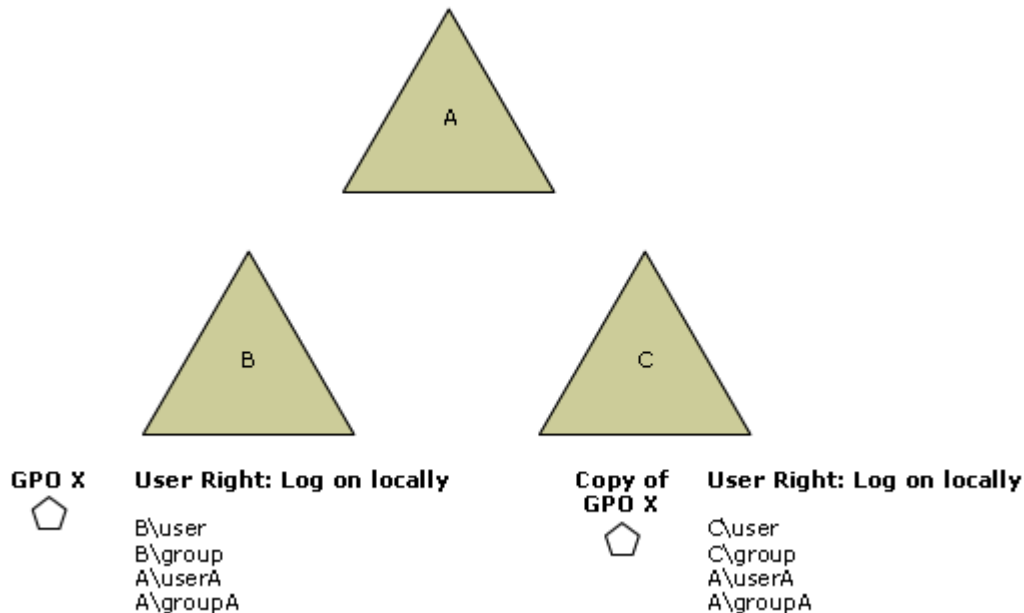
Assume for this scenario that the administrator wants to copy or import GPO X in domain B in the TEST forest to Domain E in the PRODUCTION forest. GPO X contains security settings such as the Log on locally setting under User Rights Assignment that reference security principals throughout the TEST forest. These security principals may reside in the same domain as the GPO or potentially in different domains in the TEST forest. In the drawing above, these security principals are represented as A\user, A\group, etc, where “A” is the domain, and “user” is the relative name of the security principal.

In this scenario, when copying GPO X to the new domain, the administrator will want to map all security principals that are referenced in the GPO. At a minimum, the domain prefix will need to change and potentially the relative names as well.

This scenario can be handled by using a migration table.

Production-to-production migration

The production-to-production scenario has all domains in production environments and there is a trust between the source and target domains. The diagram below assumes A, B, and C are all production domains in the same forest. Note that you could also have this scenario across forests provided there was a trust in place.



Assume for this scenario that the administrator wants to copy GPO X from production domain B to production domain C. There are potentially two alternative behaviors that are desired in this scenario:

- Retain all references to security principals in the copied GPO. Functionally, this would be equivalent to cross-linking GPO X to domain C (in terms of the settings that are applied from the GPO). This scenario is handled when you choose no migration table.
- Map some or all of the security principals to new values. For example for security principals defined in domain B, it may make sense to map them to domain C when copying the GPO from B to C. In particular, and domain local groups must be mapped. However, it probably makes sense to leave references defined in domain A as is. This scenario can also be handled using a migration table.

Creating a Staging Environment

Most administrators will want to deploy Group Policy to a test environment before introducing it to their production environment. Deploying Group Policy ideally requires the following steps:

- Gather management requirements for the target platform.
- Determine what management tasks can be done through Group Policy.
- Test Group Policy in staging environment.
- Use GPMC to migrate Group Policy to production environment.

GPMC can be used for planning, creating, testing, and migrating the Group Policy environment.

For best results, you should have a test environment that closely resembles the production environment, in terms of domains, OUs, GPOs, and groups. Using this test environment, you can test and validate changes to your policy deployment in a controlled, isolated manner that does not impact production users. Once the change has been validated, you can use the import and/or copy functions to migrate the GPOs to production.

Creating a staging environment that closely resembles the production environment is essential for this task. GPMC facilitates this by providing two sample scripts that help you create a new test environment, based on an existing environment.

- **CreateXMLFromEnvironment.wsf:** This script uses the information in a live domain to generate an XML file and a set of GPO backups that represent the policy information for that domain. The XML file captures information such as OU structure, groups and users, GPOs and the settings contained in them, links to GPOs, security on GPOs, and WMI filters. By running this script against a production domain, you can capture the essential policy information for that domain for later re-use.
- **CreateEnvironmentFromXML.wsf:** This script populates a domain with policy information such as OU structure, groups, and users, GPOs and the settings contained in them, links to GPOs, security on GPOs, and WMI filters using an XML file and a set of GPO backups referenced in the XML. The XML file required as the input for this script can be generated using the previous script. By using this second script in conjunction with the XML file previously generated, you can replicate the contents of one domain to another.

For more details on using these two scripts, see the chapter, “Staging Group Policy Deployments” in the Windows Server 2003 Deployment Kit.

WMI Filters

WMI Filters are a new feature in Windows Server 2003 and Windows XP. WMI Filters allow an administrator to dynamically determine the scope of GPOs based on attributes of the target computer. This provides the administrator with the potential to dramatically extend the filtering capabilities for GPOs well beyond the previously available security filtering mechanism.

A WMI filter is a separate object that can be linked to a GPO. When the GPO is applied on the target computer, the filter is evaluated on the target computer. A WMI filter consists of one or more queries that are evaluated against the WMI repository of the target computer. If the total set of queries evaluates to false, the GPO is not applied. If all queries evaluate to true, the GPO is applied. Each query is written using the WMI Query Language (WQL), which is a SQL-like language for querying the WMI repository.

Note that client support for WMI filters exists only on Windows XP and later operating systems. Windows 2000 clients will ignore any WMI filter and the GPO is always applied, regardless of the WMI filter.

Each GPO can have only one WMI filter. However, the same WMI filter can be linked to multiple GPOs. Like GPOs, WMI filters are per domain objects.

Figure 7 in the Scoping GPOs section shows a GPO scope pane with a link to the GPO for the “XP Systems” WMI filter. WMI filters are only available in domains that have the Windows Server 2003 configuration. Although none of the domain controllers need to be running Windows Server 2003, you must have run **ADPrep /DomainPrep** in this domain. ADPrep is a utility included on the Windows Server 2003 CD and must be run before upgrading an existing Windows 2000 domain to Windows Server 2003. If ADPrep /DomainPrep has not been run in a Windows 2000 domain, the **WMI Filters** node will not be present, and the **GPO scope** tab will not have a WMI filters section.

The user can create new WMI filters from the **WMI Filters** container in the GPMC console. Right-clicking either the **WMI Filters** container or the Contents pane for this node allows the user to create a new WMI filter or to import a filter that was previously exported. Selecting **New** will present the user with the dialog box in Figure 22.

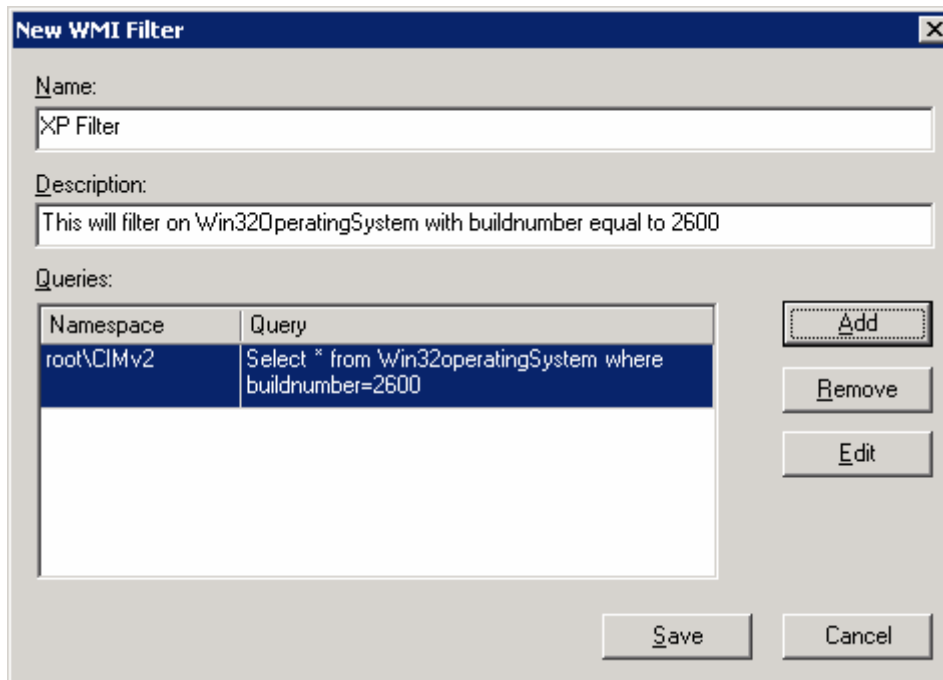


Figure 22

The user enters a name for the WMI filter, an optional description, and then one or more WQL queries using the **Add** button. Note that for each query, you must specify the WMI namespace where the query is to be executed. The default namespace is `root\CIMv2`, which should be appropriate for most scenarios. When the user presses the **Save** button, the query syntax is checked before the WMI filter can be saved.

There are three methods for linking a WMI filter to a GPO:

1. On the **Scope** tab of the GPO, use the **WMI filtering** dropdown to select a WMI filter to link to the GPO.
2. On the **General** tab of a WMI filter, right-click the **GPOs that use this WMI Filter** section and select **Add** (shown below in Figure 23). Selecting **Add** will present the user with a list of GPOs in the domain to which the user can link the WMI filter. You can only link to one GPO at a time from this pane.
3. Using drag and drop, drag a WMI filter onto a GPO.

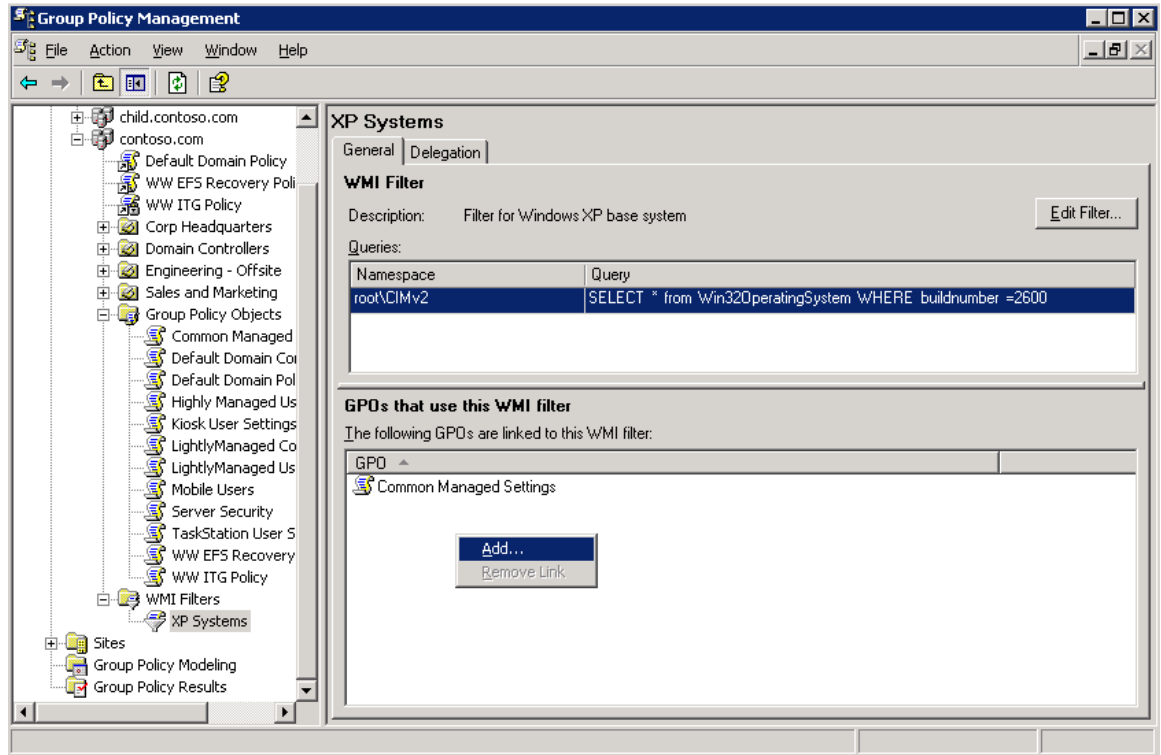


Figure 23

There is no option to link to a GPO in another domain because WMI filters can not be linked to GPOs in a different domain. Note that the ability to link a WMI filter to a GPO requires edit access to the GPO, as the link to the WMI filter is an attribute of the GPO.

The General tab on the WMI filter pane allows the user to edit a WMI filter. If the user does not have write access to the WMI filter, the **Edit Filter** button is grayed out. The user can modify the WMI Filter name, description, and the WMI query from this dialog box.

Searching for GPOs

GPMC provides extensive capabilities to search for GPOs within a domain or across all domains shown in a forest. This search feature allows you to search for GPOs based on:

- Display name of the GPO.
- Whether or not a specific domain contains links to the GPO.
- The permissions set on the GPO.
- The WMI filter that is linked to the GPO.
- The *type* of policy settings that have been set in the User Configuration or Computer Configuration in the GPO, such as folder redirection or security settings. Note that you cannot search based on the individual settings configured in a GPO.
- GUID of the GPO.

Figure 24 shows the GPO Search dialog box.

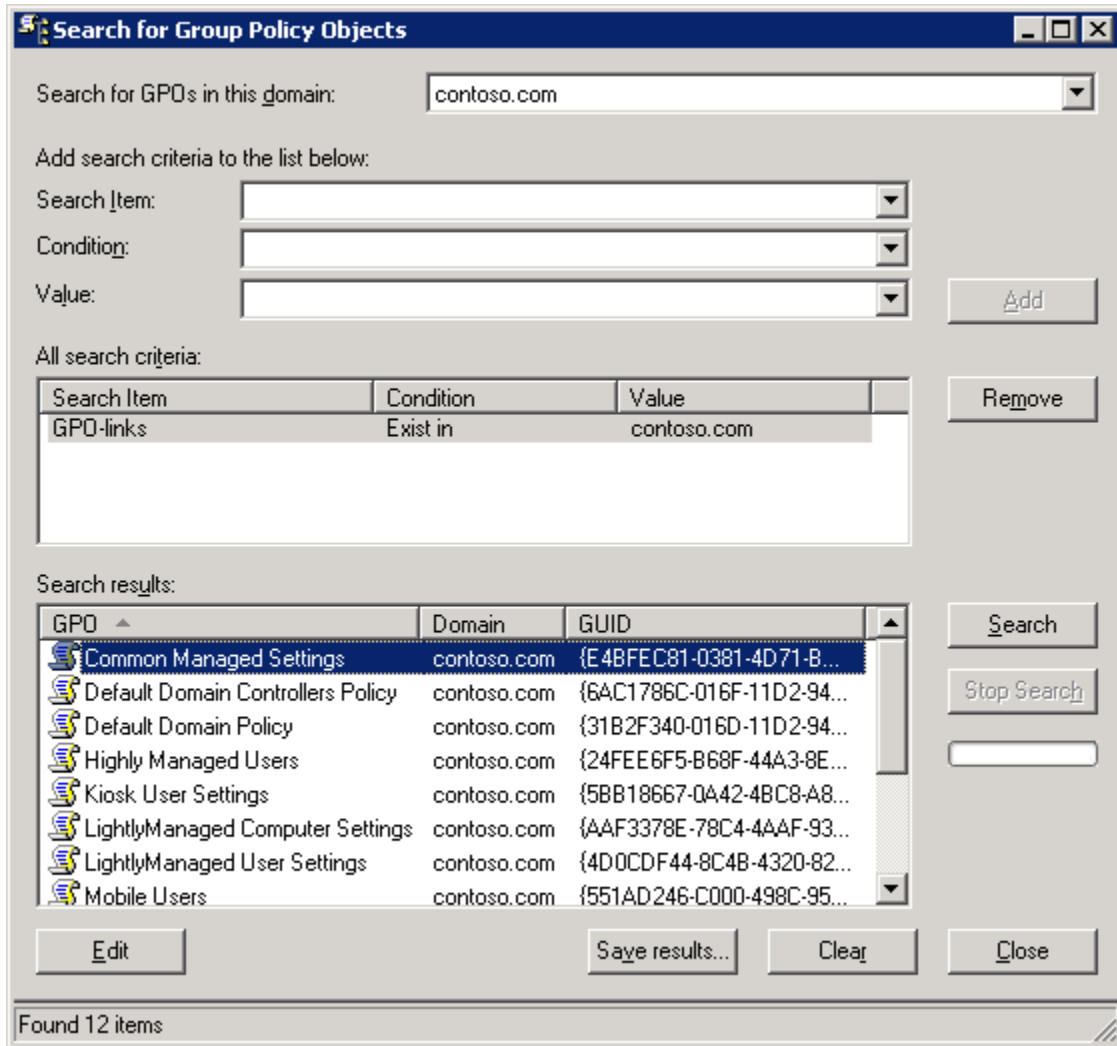


Figure 24

The GPO search by name and by GUID functions allow the user to search for a GPO by the GPO display name or by GUID associated with the GPO. The search by User Configuration or Computer Configuration allows the user to find GPOs that contain certain types of Group Policy settings. Refer to Table 3 for a list of the Group Policy settings allowed in this search feature.

The search by security group feature allows the user to find GPOs that have certain permissions applied to them. You can search for GPOs that either explicitly have these permissions (or explicitly do not have these permissions) or that have these permissions effectively applied to them (or not). An explicit permission on a GPO means the security principal is directly referenced in the ACL on the GPO. An effective permission means the security principal has permissions on the GPO either as the result of an explicit ACE, or because of its group membership. These factors combine to give a security principal the merged or effective set of permissions they have on the GPO.

Searching by GPO-Link allows the user to find unlinked or cross-domain linked GPOs. For example, if you are searching for GPOs in a given domain and you perform a search where GPO links do NOT exist in that domain, this search type will return the list of unlinked GPOs.

Searching by GPOs that link to a WMI filter allows the user to find all GPOs that link to a specified WMI filter.

Table 3 summarizes the GPO search actions and how they can be used.

Table 3

Search Item	Search Condition	Value
GPO name	Contains Does not Contain Is Exactly	GPO Display name
GPO-Link	Exist in Does not Exist in	Domain name(s) [All Sites]
Security Group	Has this explicit permission Does not have this explicit permission Has this effective permission Does not have this effective permission	Apply Settings Edit Settings Edit Settings, Delete, Modify Security Read Settings
Linked WMI filter	Is Is not	WMI Filter name
User Configuration	Contains Does not Contain	Folder Redirection Internet Explorer Branding Registry Scripts Software Installation
Computer Configuration	Contains Does not Contain	EFS Recovery IP Security Microsoft Disk Quota QoS Packet Scheduler Registry Scripts Security Software Installation Wireless Group Policy
GPO GUID	Equals	GUID

Note: When searching based on user or computer configuration, if a setting is enabled, and then all the settings in that extension are removed, there can be false-positive search for certain types of settings. This happens because the GPO has the extension listed as active. The extensions with this behavior are Security Settings, Software Installation, Folder Redirection, Internet Explorer Maintenance, and Encrypting File System (EFS).

Group Policy Modeling

Windows Server 2003 has a powerful new Group Policy management feature that allows the user to simulate a policy deployment that would be applied to users and computers before actually applying the policies. This feature, known as Resultant Set of Policy (RSOP) – Planning Mode in Windows Server 2003, is integrated into GPMC as Group Policy Modeling. This feature requires a domain controller that is running Windows Server 2003 in the forest, because the simulation is performed by a service that is only present on Windows Server 2003 domain controllers. However, with this feature, you can simulate the resultant set of policy for any computer in the forest, including those running Windows 2000.

In Figure 25, note that the Contoso.com Windows Server 2003 forest has a **Group Policy Modeling** container in the tree pane and the Tailspintoys.com Windows 2000 forest does not have this container.

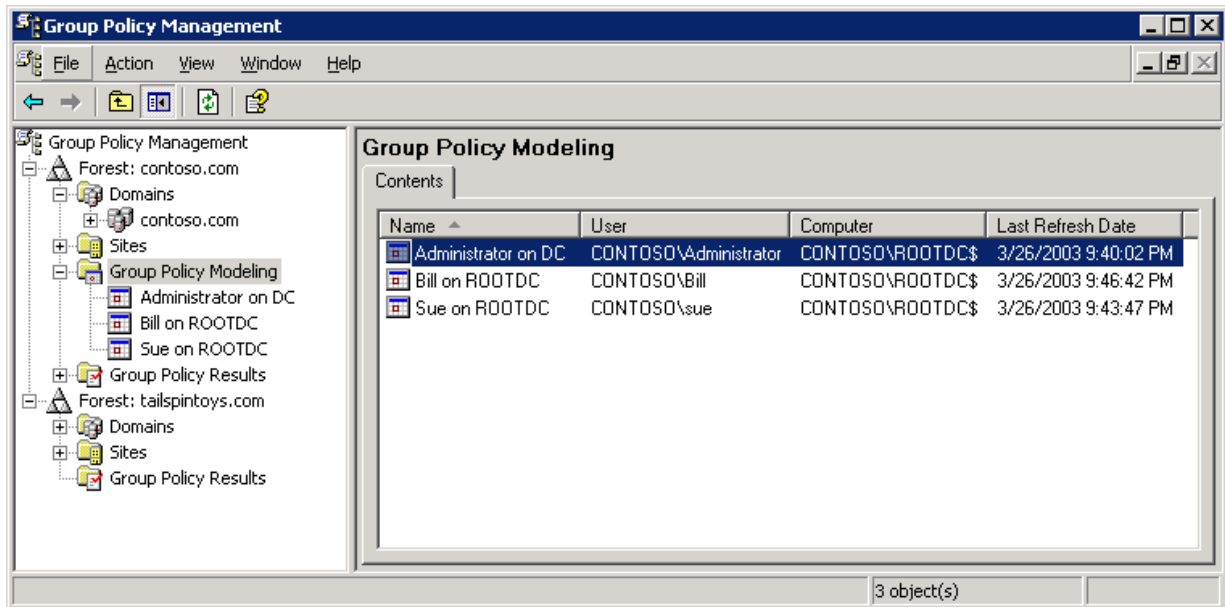


Figure 25

The contents tab on the **Group Policy Modeling** node displays a summary of all Group Policy Modeling queries that the user has performed. This is shown in Figure 25. For each query, GPMC shows the following data:

- Name – This is the user-supplied name of the modeling results.
- User – This is the user object (or the OU where the user object is located) that forms the basis of the modeling query.
- Computer – This is the computer object (or the OU where the computer object is located) that forms the basis of the modeling query.
- Last refresh time – This is the last time the planning query was refreshed.

The Group Policy Modeling Wizard can be opened from the Group Policy Modeling container, the domain node, or from any OU. When the Group Policy Modeling Wizard is started from one of the SOM

containers, the wizard automatically passes the SOM data to the wizard and pre-populates the User and Computer Selection page of the wizard.

Note: For users that are familiar with the RSoP MMC snap-in in Windows Server 2003, the Group Policy Modeling Wizard is a newer version of the RSoP wizard, running in Planning mode. Because all RSoP functionality provided by the RSoP MMC snap-in is included in GPMC, along with new functionality such as HTML reporting of RSoP data, it is recommended that users access all RSoP functionality primarily through GPMC, rather than the standalone RSoP MMC snap-in.

Figure 26 shows the Group Policy Modeling Wizard's Summary of Selections dialog box prior to running the modeling analysis. The settings in the summary pane are the answers supplied by the user while running the modeling wizard.

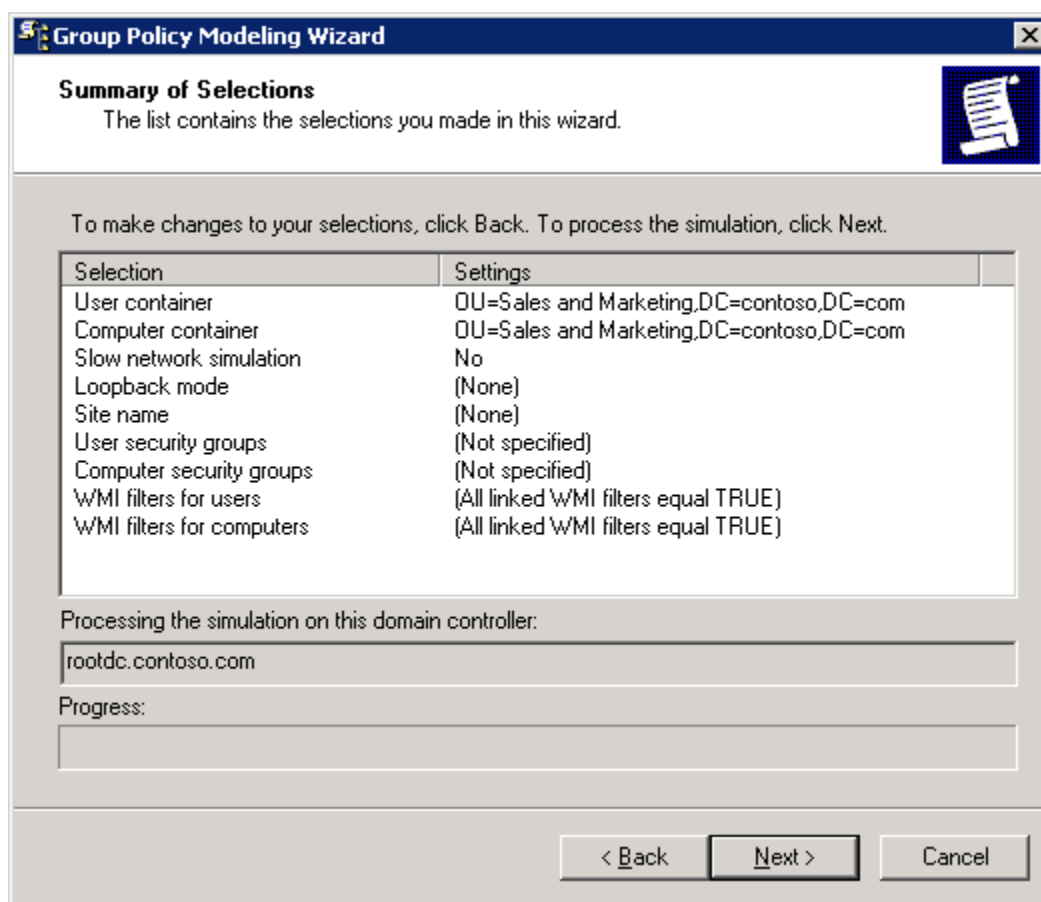


Figure 26

Once the user completes the Group Policy Modeling Wizard, a new node in the console is created to display the results. These nodes are persistent across GPMC console sessions. The user must manually remove any Group Policy Modeling nodes that are no longer desired.

For a given Group Policy Modeling query, the node contains three tabs as shown in Figure 27.

- Summary - this contains an HTML report of the summary information including the list of GPOs, security group membership, and WMI filters.

- Settings - this contains an HTML report of the simulated policy settings that would be applied in this simulation.
- Query - this lists the parameters that were used to generate the query.

Using the context menu on this new node, the user is able to:

- Save the results report to the file system. This saves the contents of both the Summary and Settings tabs as a single file (either HTML or XML).
- Re-run the query. Choosing the option to re-run the query will re-run the simulation and re-generate the data displayed in the report.
- Create a new query using the original as a template.
- Start the RSoP MMC snap-in, by choosing the "Advanced View" option. The RSoP snap-in includes the same data that is shown in the HTML report, but also shows precedence information. For example, if three GPOs set the same setting, only 1 GPO will actually set that setting. The HTML will tell you the final value and which GPO actually set it, whereas the traditional RSoP snap-in will also identify all GPOs that attempted to set that setting and the corresponding value of that setting. This is shown on the precedence tab when you double click a setting in the RSoP MMC snap-in.

The summary tab (shown in Figure 27) shows a summary of the RSoP data for the user configuration and computer configuration. For both sections, the following information is shown:

- General information including the name of the user, computer, and/or SOM for which the RSOP data was gathered.
- A list of GPOs that are in scope for the given user, computer, computer, and/or container, and the SOM to which each GPO was linked. This includes a list of GPOs that would be applied, as well as GPOs that were in scope, but would not be applied on the target.
- Simulated security group membership of the targeted user and/or computer.
- List of WMI filters that are linked to the GPOs and whether they were assumed in the query to be true or not.

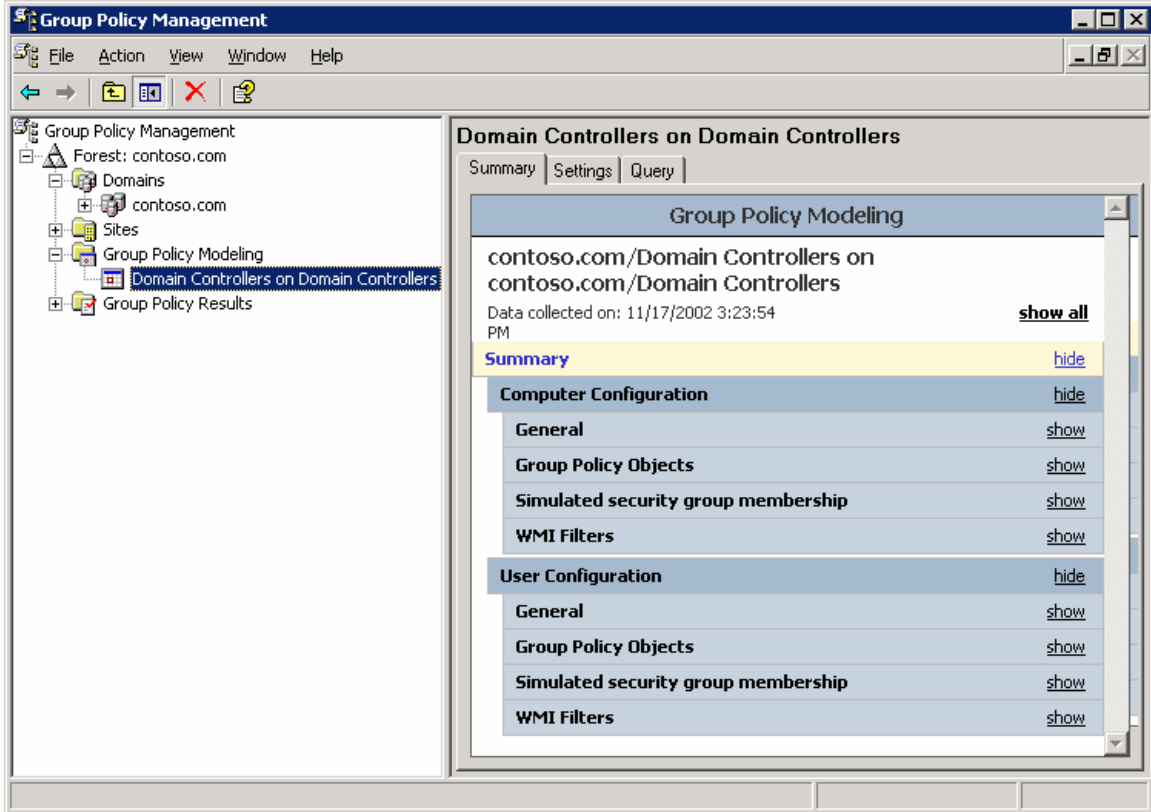


Figure 27

The settings tab (shown in Figure 28) displays a report of the final value of all policy settings that would be applied, and the GPO (for example, “Winning GPO”) that would be responsible for setting each value.

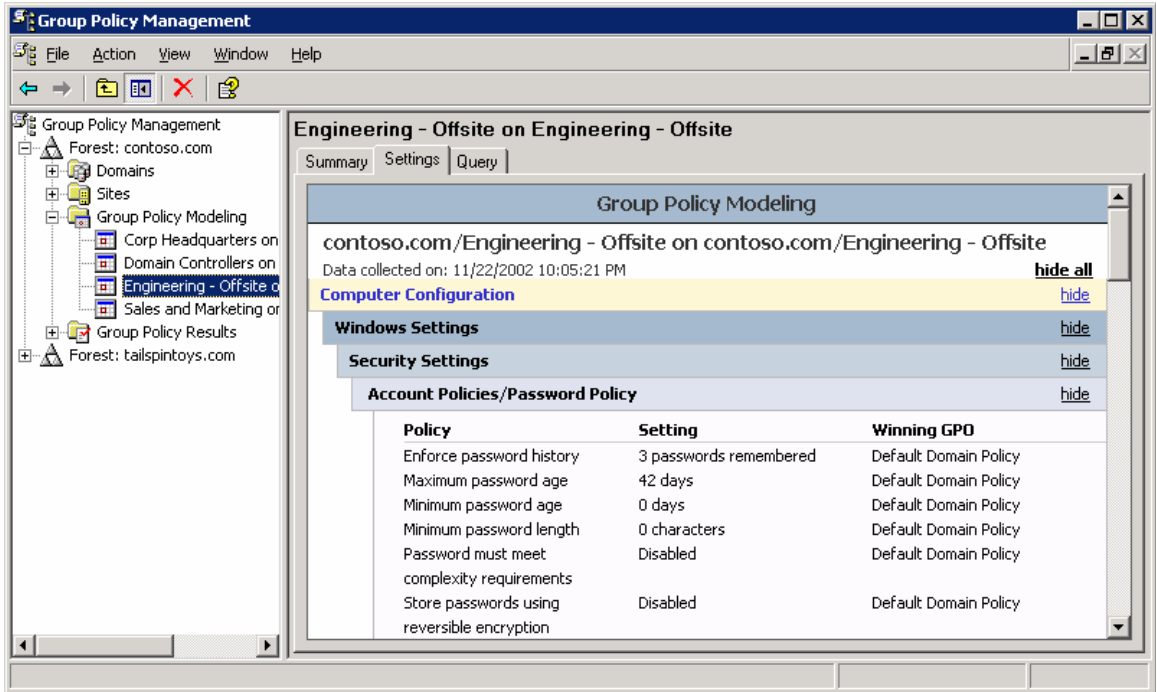


Figure 28

The query tab displays the parameters of the query entered by the user that were used to generate the data. This tab includes data that the user entered in the wizard to generate the query such as:

- Last time the query was refreshed.
- Domain controller on which the simulation was run.
- User name or SOM name for user settings.
- Computer name or SOM name for computer settings.
- If slow link processing was simulated.
- The site that the computer is assumed to be in, for this simulation.
- Whether Loopback processing was assumed, and if so, the mode (“none”, “merge mode”, or “replace mode”).
- Simulated alternate user location.
- Simulated alternate computer location.
- Simulated security group membership of user object.
- Simulated security group membership of computer object.
- WMI filters that were assumed to be true for the computer object
- WMI filters that were assumed to be true for the user object

Group Policy Results

This feature allows administrators to determine the resultant set of policy that was applied to a given computer and (optionally) user that logged on to that computer. The data that is presented is similar to Group Policy Modeling data, however, unlike Group Policy Modeling, this data is not a simulation. It is the actual resultant set of policy data obtained from the target computer. Unlike Group Policy Modeling, the data from Group Policy Results is obtained from the client, and is not simulated on the DC. The client must be running Windows XP, Windows Server 2003 or later. It is not possible to get Group Policy Results data for a Windows 2000 computer. (However, with Group Policy Modeling, you can simulate the RSoP data).

Note: Technically, a Windows Server 2003 DC is not required to access Group Policy Results. However, by default, only users with local admin privileges on the target computer can remotely access Group Policy Results data. This can be delegated to additional users (as previously described), however, the ability to delegate RSoP data is only available in Active Directory forests that have the Windows Server 2003 schema (for example, you have run ADPrep /ForestPrep) in that forest.

Each Group Policy Results query is represented by a node in the tree view under the Group Policy Results container. Each node has three tabs:

- **Summary** – this is analogous to the information shown for the corresponding tab on a Group Policy Modeling node. In particular, this page shows the component status for the various Group Policy extensions. This information tells you whether there were any issues with a particular extension and is a good place to begin troubleshooting.
- **Settings** – this is analogous to the information shown for the corresponding tab on a Group Policy Modeling node.
- **Events** – this tab shows all policy-related events from the target computer (see Figure 29). Note that to gather this data, the user performing the query must have access to remotely view the event log. By default, this access is granted to all users on Windows XP, but not on Windows Server 2003. This data is useful for troubleshooting Group Policy issues. For example if the summary report indicates that a particular Group Policy component failed to process, you may be able to determine why by looking for errors and warnings in the event log.

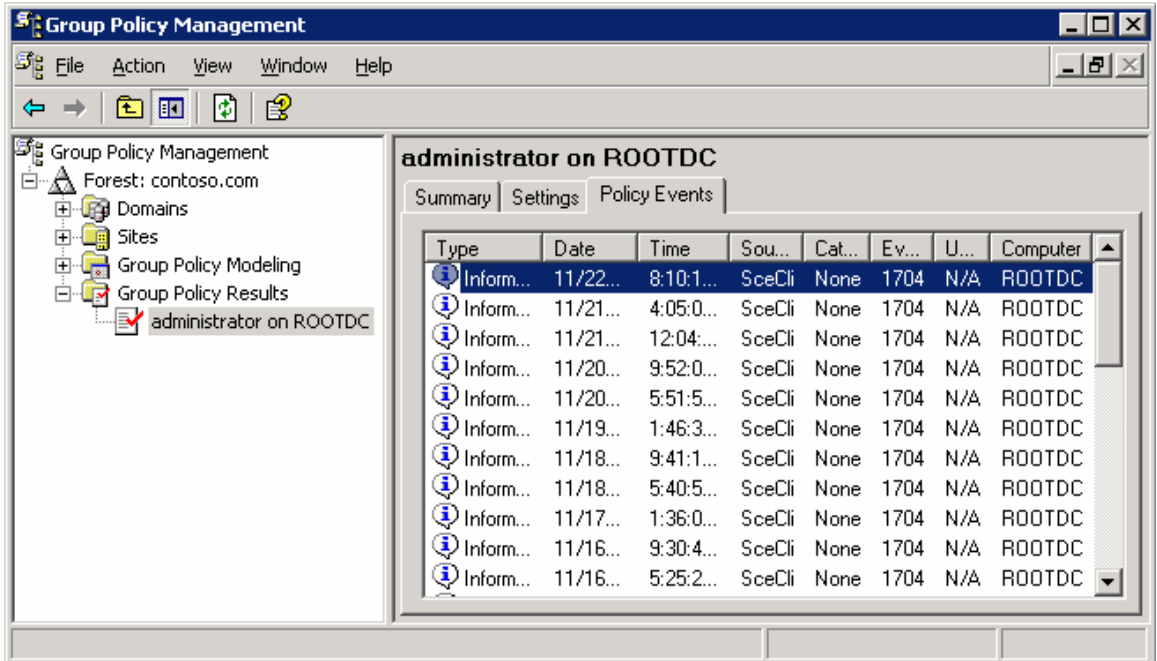


Figure 29

Platform Dependencies

GPMC exposes features that are available in the underlying operating system. Because new features have been added to Group Policy since Windows 2000, certain features will only be available in GPMC depending on the operating system that has been deployed on the domain controllers and clients. This section describes these dependencies. In general, there are four key issues that determine whether a feature is available in GPMC:

- Windows Server 2003 Active Directory schema must be available to delegate Group Policy Modeling or Group Policy Results
- Windows Server 2003 domain controller must be available to run Group Policy Modeling
- Windows Server 2003 domain configuration (ADPrep /DomainPrep) must be available to use WMI Filters
- Clients must be running Windows XP or Windows Server 2003 in order to generate Group Policy Results data.

Windows and Active Directory platform dependencies are summarized below in Table 4.

Table 4 - Group Policy Version Dependencies

Dependency	Feature	Reason
Windows Server 2003 Active Directory Schema	Delegation of Group Policy Modeling and Group Policy Results	The Generate Resultant Set of Policy (Logging) and Generate Resultant Set of Policy (Planning) permissions needed for this operation are only available with the Windows Server 2003 Active Directory schema
Windows Server 2003 Domain Controller in the forest	Group Policy Modeling	The simulation is performed by the Resultant Set of Policy Service which is only available on domain controllers running Windows Server 2003
Windows Server 2003 domain configuration (DomainPrep)	WMI Filters	ADPREP /DomainPrep configures the domain for Windows 2003 Active Directory including configuration for WMI Filters
Clients must be running Windows XP or Windows Server 2003	Group Policy Results	Clients must be instrumented to log Group Policy Results data when policy is processed. This capability is only available on the listed systems

There is no dependency from the Group Policy perspective on whether a domain is in native mode or mixed mode.

GPMC Options

The options dialog box allows the user to customize how certain features work in GPMC. The options dialog box is available from the **View** menu in GPMC. The options menu includes tabs for Columns, Reporting, and General options which allow the user to control GPMC as described below:

- Columns

This tab allows you to control the columns displayed and their order for the following list views in GPMC: **Group Policy Inheritance**, **Group Policy Objects**, **Linked Group Policy Objects** and **WMI Filters**. The columns to display can be selected by checking the appropriate column names in the **Columns** tab of the GPMC options. The order can be set by moving column names up or down in the list.

- Reporting

This tab allows you to customize the location where GPMC searches for .adm files used by reporting functions in GPMC. The reporting functions in GPMC require the .adm file for the GPO to display properly. The search location option allows the user to specify a custom search folder for the .adm files, which takes precedence over the default option of first searching the Windows folder then the SYSVOL folder of the GPO. This option is discussed further in the **Reporting on GPO Settings** section earlier in this white paper.

- General

This tab allows you to:

- Enable or disable trust detection. By default you can only add a forest to GPMC for which there is a 2-way trust with the forest of the user running GPMC. You can optionally enable GPMC to work with only 1-way trust. By using the **Stored User Names and Passwords** in Windows XP and Windows Server 2003, you can also enable access to un-trusted forests, as described earlier in the “Managing Multiple Forests” section,
- Enable or disable confirmation dialog boxes to distinguish between GPOs and GPO Links. As mentioned previously, GPMC distinguishes between GPOs and GPO-links in several ways. One method is a confirmation dialog box which appears by default when a user clicks on a GPO-link. This option controls whether that confirmation is displayed.
- Display the domain controller name beside the domain name. By default, GPMC displays the domain controller that GPMC is using for each domain in the result pane when you go to the **Domains** node in the console. Using this option you can specify that GPMC should always display the domain controller in parentheses as part of the name of the domain in the console tree.

Internet Explorer Enhanced Security Configuration Considerations

Windows Server 2003 includes a new default security configuration for Internet Explorer, called Internet Explorer Enhanced Security Configuration (ESC). ESC impacts the Security Zones and Privacy settings within the Internet Explorer Maintenance settings of a GPO. The Security Zones and Privacy settings can either be ESC enabled or not.

- When you edit settings for Security Zones and Privacy settings in a GPO from a computer where ESC is enabled, that GPO will contain ESC-enabled settings. When you look at the HTML report for that GPO, the Security Zones and Privacy header will be appended with the text **(Enhanced Security Configuration enabled)**.
- When you edit settings for Security Zones and Privacy settings in a GPO from a computer where ESC is not enabled, that GPO will contain ESC-disabled settings. ESC is not enabled on any computer running Windows 2000 or Windows XP, nor on computers running Windows Server 2003 where ESC has been explicitly disabled.

ESC settings deployed through Group Policy will only be processed on and applied by computers where ESC is enabled. ESC settings will be ignored on computers where ESC is not enabled (all computers running Windows 2000 and Windows XP, and Windows Server 2003 computers where ESC has been explicitly disabled). The converse is also true: A GPO that contains non-ESC settings will only be processed on and applied by computers where ESC is not enabled.

Furthermore, ESC impacts the functionality contained in the HTML reports produced by GPMC as follows.

- On computers with ESC enabled a prompt appears when you attempt to view reports in GPMC. This happens because the reports contain a script that allows you to expand and collapse sections of the reports using **Show** and **Hide**. To use the **Show** and **Hide** functionality in these reports, you must add the *About:security_MMC.exe* site to the Trusted Sites zone in Internet Explorer. This site represents all Web pages that are hosted inside MMC. You can do this by clicking **Add** on the **Internet Explorer** prompt. This opens the **Trusted sites** dialog box with the correct entry (*About:security_mmc.exe*) for the page being called by GPMC. Click **Add**, and then click **Close** in the **Trusted sites** dialog box to add this site to the Trusted sites zone. If the *About:security_mmc.exe* site is not added to the Trusted sites zone, the reports appear fully expanded and cannot be collapsed.
- In addition, the Explain text for a given setting in the HTML report is available by clicking on any setting in the Administrative Templates section of the GPO, assuming you have already added *About:security_MMC.exe* to the list of trusted sites. A prompt appears when you attempt to view the Explain text for a given administrative template setting in the HTML report. This prompt will ask if you want to add the *about:blank* site to the list of trusted sites. This is not recommended because it could significantly compromise the security of Internet Explorer on that computer. If you do not add the *about:blank* site to the list of trusted sites, you will not lose significant functionality in GPMC. You will still be able to view the Explain text, however, the Print and Close buttons in the Explain text dialog box will not be functional. To close the dialog, use the close box in the upper right corner.

Scripting Group Policy-related Tasks

The GPMC user interface is based on a set of COM interfaces that accomplish most of the operations performed by GPMC. These interfaces are available to Windows scripting technologies like JScript and VBScript as well as programming languages such as Visual Basic and VC++. For example, the following capabilities are scriptable using these interfaces:

- Creating/deleting/renaming GPOs.
- Linking/unlinking GPOs and WMI filters.
- Delegation:
 - Security on GPOs and WMI filters.
 - Group Policy-related security on sites, domains, OUs.
 - Creation rights for GPOs and WMI filters.
- Generating reports of GPO settings.
- Generating reports of RSOP data.
- Backup/Restore of GPOs.
- Import/Export, Copy/Paste of GPOs.
- Search for GPOs, WMI filters, SOMs, and backups.

These interfaces are discussed in detail in the GPMC software development kit (SDK) located in the %programfiles%\gpmc\scripts\gpmc.chm help file on systems where GPMC has been installed. The contents of the GPMC SDK are also available in the Platform SDK.

GPMC comes with a number of sample scripts (written mostly in VBScript but some JScript) that form a toolkit of scripts that administrators can use to directly administer a Group Policy environment or as examples to build more elaborate management tools. The scripts are installed in the %programfiles%\gpmc\scripts directory. Table 5 shows a list of scripts that are provided to do the associated types of Group Policy administrative tasks:

Table 5

Administrative task	Script name	Description
Back up a GPO	BackupGPO.wsf	Backs up all GPOs in a domain to the specified backup directory.
Back up all GPOs in a domain	BackupAllGPOs.wsf	Given a GPO name or a GUID, backs up the GPO to a specified backup directory.
Create a GPO with default options	CreateGPO.wsf	Creates a GPO with the specified name, in the current domain, using the default options.
Create a migration table	CreateMigrationTable.wsf	Populates the entries of a migration table with security principals and UNC paths that are referenced in a GPO or backup.
Copy a GPO	CopyGPO.wsf	Creates a new GPO and copies the settings from the source GPO into the new destination GPO, given a source GPO name or GUID and a new destination GPO name.
Create a policy environment using an XML representation	CreateEnvironmentFromXML.wsf	Reads an XML file that specifies a policy environment; for example, OUs, GPOs, links, and security groups. The script can either create the environment in a domain by creating the objects, or delete the environment by deleting objects specified

		in the XML file.
Create an XML representation of a policy environment	CreateXMLFromEnvironment.wsf	Reads an existing policy environment and creates an XML file representing that environment. The XML file captures information about OUs, GPOs, and GPO links, and security on GPOs. You can use this script in conjunction with the CreateEnvironmentFromXML.wsf script to create a replica of domain for staging purposes.
Delete a GPO	DeleteGPO.wsf	Deletes the specified GPO when given a GPO name or GUID. By default the script deletes links to that GPO within the same domain.
Grant Permissions for all GPOs in a Domain	GrantPermissionOnAllGPOs.wsf	Grants a user or group the specified level of permission for all GPOs in the specified domain.
Generate a report for a GPO	GetReportsForGPO.wsf	Creates an HTML and XML report for a given GPO at a given location in the file system.
Generate a report for all GPOs in the domain	GetReportsForAllGPOs.wsf	Creates HTML and XML reports for all GPOs in the domain, at a given location in the file system.
Import settings into a GPO	ImportGPO.wsf	Imports the settings from the specified backup to the existing destination GPO in the domain
Import multiple GPOs into a domain	ImportAllGPOs.wsf	Creates a new GPO and imports settings into that GPO for each backed-up GPO stored at a specific file system location.
Restore a GPO	RestoreGPO.wsf	Restores a backed-up GPO.
Restore all GPOs	RestoreAllGPOs.wsf	Restores all GPOs that are stored at a given file system location
Grant permissions for GPOs linked to a domain, OU, or site	SetGPOSecurityBySOM.wsf	Grants a user or group the specified permission type for all GPOs that are linked to a specified domain, OU, or site. You can specify Read , Apply , Edit , FullEdit , or None for the permission type.
Set GPO permissions	SetGPOPermissions.wsf	Sets the permission level for a security principal on a given GPO. You can specify Read , Apply , Edit , FullEdit , or None for the permission type.
Set permissions to create GPOs	SetGPOCreationPermissions.wsf	Grants or removes the ability to create GPOs in a domain for a given security principal.
Set policy-related permissions on a given site, domain, or OU	SetSOMPermissions.wsf	Sets policy-related permissions on a given scope of management (SOM). A SOM is any site, domain, or OU.
List all GPOs in a domain	ListAllGPOs.wsf	Prints all GPOs in the specified domain.
List disabled GPOs	FindDisabledGPOs.wsf	Prints all GPOs in the specified domain that are disabled or partially disabled.
List GPO information	DumpGPOInfo.wsf	Prints the information for a specific GPO, including creation time, modification time, owner, status, version number, links, security groups that filter the

		GPO, and security groups that have full control, edit, read, or custom permissions.
List scope of management information	DumpSOMInfo.wsf	Prints all information for a specific Scope of Management (SOM), including GPO links and policy related permissions on the SOM. A SOM is any site, domain, or OU.
List GPO by policy extension	FindGPOsByPolicyExtension.wsf	Prints all GPOs in the specified domain for which a specific policy extension is configured; for example, find all GPOs that contain the Software Installation or Folder Redirection policy settings.
List GPOs by security group	FindGPOsBySecurityGroup.wsf	Prints all GPOs that for which a given security principal has the specified permission on that GPO. You can specify Read , Apply , Edit , or Fulledit for the permission type.
List GPOs with duplicate names	FindDuplicateNamedGPOs.wsf	Prints all GPOs in the specified domain that have duplicate names.
List GPOs without Apply permission	GPOsWithNoSecurityFiltering.wsf	Prints all GPOs in the specified domain that do not apply to anyone because Apply permission is not set on the GPO.
List GPOs Orphaned in SYSVOL	FindOrphanedGPOsInSYSVOL.wsf	Finds and prints all GPOs in SYSVOL with no corresponding component in Active Directory.
List domains and OUs with external GPO links	FindSOMsWithExternalGPOLinks.wsf	Prints all domains and OUs in the specified domain that link to a GPO in a different domain.
List unlinked GPOs in a domain	FindUnlinkedGPOs.wsf	Prints all GPOs in the specified domain that have no links. Links outside the domain, including site links, are not checked.
Print the scope of management policy tree	ListSOMPolicyTree.wsf	Prints all SOMs in the specified domain with the list of GPOs that are linked to the domain and each OU.
List GPO backups in a given file system location	QueryBackupLocation.wsf	Prints information about all backed up GPOs at the file system location specified by the user.

All of the scripts are intended for command line operation. The user can execute a script using the following command (using the CreateGPO script as an example) from a command shell:

```
Cscript CreateGPO.wsf
```

Alternatively, you can set Cscript to be the default scripting engine by using this command:

```
cscript //H:cscript
```

The user will need to run the scripts from the %programfiles%\gpmc\scripts directory or by specifying the path to the scripts directory. To see usage details for any script, use the “/?” command line option.

Related Links

See the following resources for further information:

- [Enterprise Management with the Group Policy Management Console](http://www.microsoft.com/windowsserver2003/gpmc/default.mspx) at <http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>.
- [Migrating GPOs Across Domains with GPMC](http://www.microsoft.com/windowsserver2003/gpmc/migrppo.mspx) at <http://www.microsoft.com/windowsserver2003/gpmc/migrppo.mspx>.

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003) at <http://www.microsoft.com/windowsserver2003>.

For information about Group Policy in general see <http://www.microsoft.com/grouppolicy>. TechNet also features a Group Policy page at <http://www.microsoft.com/technet/grouppolicy>.